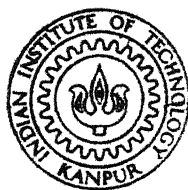# EIGEN - STRUCTURE OF REED - MULLER MATRICES AND REED - MULLER EXPANSIONS OF BOOLEAN FUNCTIONS

By

Major V N MONEY

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR
FEBRUARY, 1985

EIGEN - STRUCTURE OF REED - MULLER MATRICES AND REED - MULLER EXPANSIONS OF BOOLEAN FUNCTIONS

A Thesis Submitted

In Partial Fulfilment of the Requirements

for the Degree of

MASTER OF TECHNOLOGY

By

Major V N MONEY

to the

DEPARTMENT OF ELECTRICAL ENGINEERING

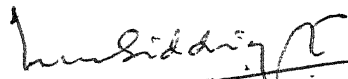INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

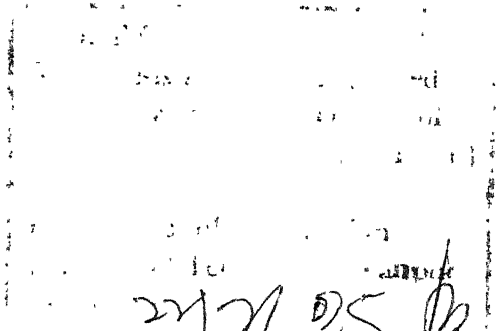FEBRUARY, 1985

87600

EE-2585-M-MON-EIG

CERTIFICATE

Certified that this work 'EIGEN STRUCTURE, OF REED –
MULLER MATRICES AND REED-MULLER EXPANSIONS OF BOOLEAN
FUNCTIONS', carried out by Major V.N. Money under my
supervision has not been submitted elsewhere for a degree.

Feb. 1985

(M.U. Siddiqi)
Assistant Professor
Department of Electrical Engineering
Indian Institute of Technology
Kanpur

ACKNOWLEDGEMENT

ABSTRACT

A Boolean function may be expressed, using Exclusive
OR, AND, and NOT gates, in an unique canonical form, called
Reed-Muller expansion, which is similar to minterm expansion
of a Boolean function. The expansion with Exclusive-OR gates
possesses inherent advantages over conventional realisation
of Boolean functions. Minimisation of Exclusive-OR gates,
to suit optimal design conditions, consists of obtaining what
is known as the polarity function of the coefficients in Reed-
Muller expansions; polarity function gives logical conditions
of the input variables. Transformations of minterm coeffi-
cients to the coefficients in Reed-Muller expansions, being
linear, are represented by matrices, called Reed-Muller
matrices. Reed-Muller matrices are factorised using direct -
product & Good's techniques, which facilitates handling of
these matrices in the computer. Algorithmic methods for
finding the eigen-structure of Reed-Muller matrices, using
the concepts of the null-space, generalised inverses of
matrices, have been evolved and utilized for the genera-
tion of coefficients in Reed-Muller expansions from which
one can obtain polarity functions for the minimum
expansion.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 SCOPE OF WORK:

An attempt has been made in this thesis to study the eigenstructure of Reed-Muller matrices and utilize their structure for generation of Reed-Muller expansion coefficients of Boolean functions. An alternative procedure based on factorization of Reed-Muller matrices, using Good's techniques, has also been given for the generation of Reed-Muller expansion coefficients.

Any Boolean function may be expressed in a sum(s)-of-product canonical form. Employing only Exclusive-OR (Ex-OR) gate and AND gates and by algebraic substitution and simplification this may be uniquely represented by a similar canonical form [1],[2]. As an example, a 3 variable function of (x_3, x_2, x_1) is considered. The minterm expansion, using AND gates, OR gates and NOT gates of this function is

$$f(x_3, x_2, x_1) = c_0 \, \bar{x}_3 \bar{x}_2 \bar{x}_1 + c_1 \, \bar{x}_3 \bar{x}_2 x_1 + c_2 \, \bar{x}_3 x_2 \bar{x}_1 + c_3 \, \bar{x}_3 x_2 x_1$$

$$+ c_4 \, x_3 \bar{x}_2 \bar{x}_1 + c_5 \, x_3 \bar{x}_2 x_1 + c_6 \, x_3 x_2 \bar{x}_1 + c_7 \, x_3 x_2 x_1$$

$$(1.1)$$

where $c_i \{0,1\}$ depending on the function value of the related input variables. Every OR gate in the above expression may be replaced by an Ex-OR gate as only one minterm becomes 1 for every combination of values x_3, x_2, x_1 and others 0. The equivalent expression, therefore, may be written as

$$f(x_3, x_2, x_1) = c_0\, \bar{x}_3\bar{x}_2\bar{x}_1 \oplus c_1\, \bar{x}_3\bar{x}_2 x_1 \oplus c_2\, \bar{x}_3 x_2 \bar{x}_1 \oplus c_3\, x_3 x_2 x_1$$
$$\oplus c_4\, x_3\bar{x}_2\bar{x}_1 \oplus c_5\, x_3 x_2 \bar{x}_1 \oplus c_7\, x_3 x_2 x_1$$

$$(1.2)$$

and substituting the identity $\bar{x}_i = 1 \oplus x_i$, the expansion is obtained in the following form

$$f(x_3, x_2, x_1) = c_0(1 \oplus x_3)(1 \oplus x_2)(1 \oplus x_1) \oplus c_1(1 \oplus x_3)$$
$$(1 \oplus x_2)\, x_1 \oplus c_2(1 \oplus x_3) x_2(1 \oplus x_1) \oplus c_3(1 \oplus x_3)$$
$$x_2 x_1 \oplus c_4\, x_3(1 \oplus x_2)(1 \oplus x_1) \oplus c_5\, x_3(1 \oplus x_2)\, x_1$$
$$\oplus c_6\, x_3 x_2(1 \oplus x_1) \oplus c_7\, x_3\, x_2\, x_1$$

$$(1.3)$$

which reduces to

$$= c_0 \oplus (c_0 \oplus c_1) x_1 \oplus (c_0 \oplus c_2)\, x_2$$
$$\oplus (c_0 \oplus c_1 \oplus c_2 \oplus c_3) x_2 x_1 \oplus (c_0 \oplus c_4)\, x_3$$
$$\oplus (c_0 \oplus c_1 \oplus c_4 \oplus c_5)\, x_3 x_1 \oplus$$

$$(c_0 \oplus c_2 \oplus c_4 \oplus c_6)x_3 x_2 \oplus (c_0 \oplus c_1 \oplus$$

$$c_2 \oplus c_3 \oplus c_4 \oplus c_5 \oplus c_6 \oplus c_7)\ x_3 x_2 x_1$$

$$= a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_2 x_1 \oplus a_4 x_3 \oplus$$

$$a_5 x_3 x_1 \oplus a_6 x_2 \oplus a_7 x_3 x_2 x_1 \tag{1.4}$$

where

$$a_0 = c_0$$
$$a_1 = c_0 \oplus c_1$$
$$a_2 = c_0 \oplus c_2$$
$$a_3 = c_0 \oplus c_1 \oplus c_2 \oplus c_3$$
$$a_4 = c_0 \oplus c_4$$
$$a_5 = c_0 \oplus c_1 \oplus c_4 \oplus c_5$$
$$a_6 = c_0 \oplus c_2 \oplus c_4 \oplus c_6$$
$$a_7 = c_0 \oplus c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus c_5 \oplus c_6 \oplus c_7$$

$$\tag{1.5}$$

and $a_i \{0,1\}$ are constant coefficients that are determined by the value of the function for each combination of values x_3, x_2, x_1. As there are no complemented variables in (1.4), this is also termed as a polynomial expansion. This expansion is unique because the expansion with Ex-OR and minterm is unique and the conversion to the expansion with a_is as the coefficients is also unique.

Thus any m variable Boolean function may be expressed as a polynomial expansion. These are also known as positive - canonic or complement free Reed-Muller (CFRM) expansions of 2^m terms [3],[4]. In general, the expansion may be written as

$$f(x_1, x_2, \ldots, x_m) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots a_{2^m-1} x_1 x_2 \ldots, x_m$$

(1.6)

By complementing any variable a non-positive canonic expansion also called as the generalised Reed-Muller (GRM) expansion may be obtained, and is written as

$$f(\dot{x}_1, \dot{x}_2, \dot{x}_3 \ldots \dot{x}_m) = a_0 \oplus a_1 \dot{x}_1 \oplus a_2 \dot{x}_2 \oplus \ldots a_{2^m-1} \dot{x}_1 \dot{x}_2 \dot{x}_3 \ldots \dot{x}_m$$

(1.7)

where each $\dot{x}_i$ input variable may appear in positive or negative form but not in both forms.

Hence, an m variable Boolean function may possess 2^m different positive and non-positive canonic RM expansions, depending on the polarity of the input variables, which may be called as the polarity function of the variables of the function. Using the following identities it is possible to obtain any non-positive canonic expansion from either the positive canonic or any other non-positive canonic RM expansions.

$$x_i = 1 \oplus \bar{x}_i \qquad \text{and} \qquad \bar{x}_i = 1 \oplus x_i$$

$$1 \oplus 1 = 0 \qquad\qquad \overset{\circ}{x}_i \oplus \overset{\circ}{x}_i = 0 \qquad (1.8)$$

Suppose the positive canonic expansions in 3 variables is given as

$$f(x_3, x_2, x_1) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_2 x_1 \oplus a_4 x_3$$
$$\oplus a_5 x_3 x_1 \oplus a_6 x_3 x_2 \oplus a_7 x_3 x_2 x_1 \qquad (1.9)$$

then the expansion with polarity function 110 may be obtained by the substitution of $x_1 = 1 \oplus \bar{x}_1$, and therefore obtain

$$f(x_3, x_2, \bar{x}_1) = (a_0 \oplus a_1) \oplus a_1 \bar{x}_1 \oplus (a_2 \oplus a_3) \ x_2 \oplus a_3 x_2 \bar{x}_1$$
$$\oplus (a_4 \oplus a_5) x_3 \oplus a_5 x_3 \bar{x}_1 \oplus (a_6 \oplus a_7) \overset{\cdot}{x}_3 x_2 \oplus$$
$$a_7 \ x_3 x_2 \bar{x}_1$$
$$(1.10)$$

Where a_is are the coefficients of the positive canonic RM expansions. Allowing the coefficients of this expansion to be denoted as a_i^1 , (the decimal superscript devoting the decimal value of the binary, which represents the variables being complemented) these coefficients may be expressed in terms of the minterm coefficients as

$$a_0{}^1 = a_0 \oplus a_1 = c_1$$
$$a_1{}^1 = a_1 \qquad = c_0 \oplus c_1$$

$$a_2^1 = a_2 \oplus a_3 = c_1 \oplus c_3$$

$$a_3^1 = a_3 = c_0 \oplus c_1 \oplus c_2 \oplus c_3$$

$$a_4^1 = a_4 \oplus a_5 = c_1 \oplus c_5$$

$$a_5^1 = a_5 = c_0 \oplus c_1 \oplus c_4 \oplus c_6$$

$$a_6^1 = a_6 \oplus a_7 = c_1 \oplus c_3 \oplus c_5 \oplus c_7$$

$$a_7^1 = a_7 = c_0 \oplus c_1 \oplus c_2 \oplus c_3 \oplus c_4$$
$$\oplus c_5 \oplus c_6 \oplus c_7$$

$$(1.11)$$

The constant coefficients a_is of the positive/non-positive canonic RM expansion are respectively called as positive/non-positive canonic RM expansion coefficients or RM/GRM expansion coefficients also. The constant coefficients c_is, of the minterm expansion is accordingly, called as the minterm expansion coefficient or merely minterm coefficients.

The classical problem in switching theory has been the realisation of a switching function with minimum number of logical circuit elements. Karnaugh map and Quine-McClusky's algorithms have helped obtain a limited minimum conditions. Besides these algorithms, decomposition and other techniques have been employed to achieve economical multilevel expressions for switching functions [5], [6]. Geometric formats like

the mapping of the positive-canonic RM expansion coefficients
are used to generate any Ex-OR realisation [7] and thus try
and obtain a minimum Ex-OR design. Boolean realisations use
AND/OR/NAND and NOR gates, whereas these same functions can
also be implemented using Ex-OR/AND/NOT gates.

The advantages of Ex-OR logic design are that more
economical realisation in terms of the number of gates and
the number of gate interconnections are possible; also, designs
with Ex-OR gates facilitate easier testing in comparison
with vertex networks since the change of any input to an Ex-OR
gate will propogate a change to the output, unlike the
the vertex Boolean realisation which require specific input
pattern changes to sensitise a path to the output [8].
However, the testability advantage may even exceed the
possible disadvantage of the cost factor in the Ex-OR
realisation.

The mapping of the minterm coefficients onto the
RM expansion coefficients may be considered as the mapping
of the vector space C to a vector space A over the binary
field F. As this mapping may be written as a set of n equations
in n variables viz. the a_is and where $n = 2^m$, m being the
number of variables in the Boolean function, the mapping may
be considered as a linear transformation $T:C \rightarrow A$, which

satisfies the condition $(g\ c_x \oplus h\ c_y)\ T = g(c_x T) \oplus h(c_y T)$,
for all vectors c_x and c_y in C and all scalars g,h in F, viz.
0,1. If $c_1, c_2, \ldots c_n$ is any basis of the vector space C and
$a_1, a_2 \ldots a_n$ are any vectors in A, then there is one and only
linear transformation $T:C \to A$ with $c_1 T = a_1, \ldots, c_n T = a_n$ [9].
Allowing i_i to be the unit vectors, $i_1 = (1,0,\ldots 0)$, $\ldots$
$i_n = (0,0,\ldots 1)$ of the vector space C, then each a_i may be
written as

$$i_1 T = a_1 = (r_{11}, r_{12}, \ldots, r_{1n})$$
$$i_2 T = a_2 = (r_{21}, r_{22}, \ldots, r_{2n})$$
$$\bullet$$
$$\bullet$$
$$\bullet$$
$$i_n T = a_n = (r_{n1}, r_{n2}, \ldots r_{nn}) \qquad (1.12)$$

and therefore there is just one linear transformation
associated with (1.12) and this transformation is determined
by the nxn matrix $R = (r_{ij})$. Therefore there is a one-to-one
correspondence between the linear transformation $T:C \to A$ and
the nxn matrix R, with entries from the binary field F.
Given T, the corresponding matrix R is the matrix with ith
row, the row of co-ordinates $i_i T$; given $R = (r_{ij})$, T is the
unique linear transformation carrying each unit vector i_i
of C into the ith row $(r_{i1}, r_{i2} \ldots r_{in})$ of A.

Therefore, the processing of the minterm coefficients c_is may be expressed in the matrix form; by allowing the minterm coefficients and the GRM expansion coefficients to be column vectors; this may be written as

$$a = Rc \qquad (1.13)$$

where R is a constant matrix, called as the Reed-Muller matrix, with matrix multiplication operation being modulo 2, as all operations are over GF(2). The example of the 3 variable Boolean function may be written as

$$
\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix}
=
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}
$$

$$
=
\begin{bmatrix}
c_0 \\
c_0 \oplus c_1 \\
c_0 \oplus c_2 \\
c_0 \oplus c_1 \oplus c_2 \oplus c_3 \\
c_0 \oplus c_4 \\
c_0 \oplus c_1 \oplus c_4 \oplus c_5 \\
c_0 \oplus c_2 \oplus c_4 \oplus c_6 \\
c_0 \oplus c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus c_5 \oplus c_6 \oplus c_7
\end{bmatrix}
$$

The RM matrix for the positive canonic RM expansion may also be iteratively built up from [10].

$$R_{m'+1} = \left[\begin{array}{c|c} R_{m'} & 0 \\ \hline R_{m'} & R_m^r \end{array}\right] \quad R_o = [1] \qquad (1.14)$$

where m' = m-1, for the m variable Boolean function.

In a similar fashion, it must be feasible to obtain the RM matrices for the non-positive canonic RM expansions. The scheme developed is not an iterative one as in (1.14) but the matrix is obtained as a direct-product of two kinds of matrices of order 2x2. These matrices are termed as core matrices. The core matrix associated with a positive polarity variable is the 2x2 matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and the one associated with the complemented variable is $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. RM matrices for the non-positive canonic RM expansions are thus obtained as a direct-product of a combination of these two kinds of core - matrices, combined as per the polarity function of the variables in the Boolean function. RM matricies may also be factorised using Good's technique.

Based on the manner in which the RM matrices may be factorised two classes of RM matrices may be had viz., the RM matrix for the positive canonic RM expansion and for the non-positive canonic RM expansions. Salient features of the RM matrices observed are:

i) the RM matrix for the positive canonic RM expansion is involutary.

ii) the roots of the characteristic equation of the RM matrix, for the positive canonic RM expansion, is in the GF(2)

iii) the roots of the characteristic equation of the RM matrix is repetative

iv) the characteristic equation of the RM matrix, for the non-positive canonic RM expansions, is a product of second degree irreducible polynomial,

v) the roots of the characteristic equation of the RM matrix, for the non-positive canonic RM expansions, are therefore to be found in the extension field also,

vi) the number of kinds of roots being limited to the elements of the extension field, the roots of the characteristic equation of the RM matrix, for the non-positive canonic RM expansion, is also repetitive.

The characteristic roots are found from the characteristic equation of the matrices, and therefore, if characteristic roots are obtained as direct product of eigenvalues of the core-matrices, from which the RM matrices are constructed,

then it is possible to construct the characteristic equation from these characteristic roots. The characteristic roots are known as eigen-values also.

Every eigen-value has an eigen-vector corresponding to it. When the roots of the characteristic equations are repetitive, unique eigen-vectors for each repetitive root can not be found by the normal procedures. Two methods of obtaining the modal matrix, the matrix whose columns are the set of linearly independent (LIN) eigen-vectors of a matrix, have been outlined. In one, the concept of generalised inverses of matrices is used, and in the other the concept of null-space of a matrix is employed. The second method has been suitably adopted, for the RM matrix for the positive canonic RM expansion, and a simplified procedure has been evolved.

Having obtained the eigen structure of the RM matrices, algorithms to generate the expansion coefficients from the given truth-table of a Boolean function, have been evolved. The algorithm for the positive-canonic RM expansion makes use of the eigen-vectors of the RM matrix and relates all possible minterm coefficients to its corresponding expansion coefficients. The set of eigen-vectors forms a subgroup of the group of all possible minterm coefficients and therefore, cosets may be formed and these minterm coefficients may

now be associated to the corresponding expansion coefficients through the eigen-vectors. The other algorithm makes use of the eigen-values for generation of the non-positive canonic RM expansion coefficients. Good's technique for factorisation of RM matrices may also be used for the generation of the RM expansion coefficients.

A geometric mapping of the positive canonic RM expansion coefficients, called as 'b$_j$ maps' , has been developed to generate all non-positive canonic RM expansion coefficients [7]. However, the map operations become difficult when the number of variables in the Boolean function increases beyond 6. A computer method has been developed, to generate all non-positive canonic RM expansion coefficients from the positive canonic RM expansion coefficients [10].

1.2 LINE OF APPROACH:

The RM matrices were defined in the previous section. The RM matrix are constructed as direct product of core-matrices. Another method of factorising the RM matrix based on Good's technique is also considered. They are classified as RM matrix, for the positive canonic RM expansion and the RM matrices for the non-positive canonic RM expansions. The generalisation is based on polarity function of the variables in the Boolean function.

The eigen-structure of the RM matrices would be different for different structure of the RM matrices. It has been possible to define the number of eigen-values of the RM matrices as a function of the total number of variables of the Boolean function and the number of variables of these that appear complemented. Hence, eventhough the eigen-values of two different polarity functions may be same, as the number of variables and the number of variables being complemented being the same for two different polarity functions, the eigen-vectors of the RM matrices with these two polarity function would not be the same. The RM matrices are obtained, as direct product of the core matrices, in sequence as per the pattern of the polarity function and hence the RM matrices for different polarity functions would be different and so would the eigen-vectors be.

A Boolean function is expressed in binary and if it is not possible to obtain the eigen-values in the binary field GF(2), then the roots are found in its extension field. The characteristic equations of the RM matrices, for the non-positive canonic RM expansion, being a product of an irreducible polynomial of degree 2, it is only natural to expect the roots of the characteristic equations to be repetitive, being confined to the elements of the field. The method of

obtaining the eigen-vectors when repetitive roots occur is based on the generalised inverse of the characteristic matrices. A specific technique has been developed in this thesis to find the modal matrix of the RM matrix for the positive-canonic RM expansion.

Eigen-structure of any matrix characterises the transform. The eigen-vectors of the RM matrix for the positive canonic RM expansion, partitions the vector space C, the vector space of all possible sets of the minterm coefficients c_is. With the set of eigen-vector as a subgroup, cosets have been formed of this vector space C. By identifying the coset-leader and associating the coset-leader with an eigen-vector, through the characteristic matrix, the minterm coefficient is related to its corresponding positive canonic RM expansion coefficients. Similarly, the eigen-values of the RM matrix, for the non-positive canonic RM expansion, have been associated with the characteristic matrix and the minterm coefficients, to generate the non-positive canonic RM expansion coefficients.

1.3 OUTLINE OF THE THESIS:

In this chapter the aim of this thesis and the common terms used in this thesis were explained. The line of approach towards the generation of the RM expansion coefficients

was also given. The study of the eigen-structure itself was considered important because some input vectors remain unaltered by the transformation, except by a scaling factor, called the eigen-values. These input vectors are called as the eigen-vectors and they characterise the transformation and these could be put to appropriate use.

Chapter 2 is a mathematical recaptulation of the preliminaries necessary in the development of this thesis and highlights some techniques for obtaining the eigen-vectors.

In the next chapter, Chapter 3, the structure of the RM matrices have been studied and has been represented as direct product of core matrices. Properties of direct product of matrices have been applied to find the eigen-values of the RM matrices. The direct-product method of finding the eigen-values of the RM matrices, for the non-positive canonic RM expansion, from the eigen-values of the core matrices have been simplified into formulae. Characteristic equations of the RM matrices, from the eigen-values so obtained, has also been outlined. A simple method of finding the modal matrix of the RM matrix, for the positive-canonic RM expansion, has also been developed in this chapter. To obtain the modal matrix of the RM matrices, for the non-positive canonic RM expansion, the generalised inverse of the characteristic,

matrix, especially when the roots of the characteristic equation are repetitive, has been suitably adopted. The RM matrix has also been factorised using Good's technique.

In Chapter 4, the minimisation of the Ex-OR design has been discussed. Algorithm for generation of the positive canonic RM expansion coefficients and non-positive canonic RM expansion coefficients, directly from the minterm coefficients have been given. These algorithm are based on the eigen-vectors of the RM matrices and the eigen-values of the RM matrices respectively. Based on Good's technique of matrix factorisation sequential (binary/decimal) generation of all RM expansion coefficients has also been done.

The last chapter summarises the work in this thesis. Suggestions for further work in this field has also been given in this chapter.

CHAPTER 2

MATHEMATICAL PRELIMINARIES

This chapter briefly outlines the mathematical pre-
requisites. These include relevant results from the theory
of groups, rings, fields and matrices. Matrices not only
simplify the analysis but help in organising computer methods
for the techniques developed. Here the algebra of matrices
essential for the thesis has also been included. Standard
results have been adopted from a number of text books, a
few of these are [9],[12],[13],[14],[15],[16],[17],[18],
[19],[20].

2.1 GROUPS, RINGS AND FIELDS:

2.1.1 Groups:

A group is a set of elements with one operation and
its inverse, such as addition and its inverse viz. subtraction
and multiplication and its inverse viz. division. A group G
thus is a set of objects for which an operation is defined
and for which the following rules hold. Let a,b,c be
elements of the group. The operation is a single valued
function of two variables, say $f(a,b) = c$, which is
denoted as $a + b = c$ or $ab = c$ and called as addition or

multiplication even though it may not be addition or multiplication of the arithmetic of ordinary numbers.

Rule 1(Closure): The operation can be applied to any two group elements to give a third group element.

Rule 2 (Associative Law): For any three elements a,b and c of the group, (a+b)+c = a+(b+c) if the operation is written as addition , or a (bc)=(ab)c if the operation is written as multiplication.

Rule 3: There is an identity element. If the operation is addition, the identity elemnt is called zero, 'O' and if the operation is multiplication, the identity element is one, '1'.

Rule 4: Every element of the group has an inverse element. If the operation is addition, the inverse element corresponding to 'a' is '-a' and is defined by the equation as a+(-a) = (-a)+a=0. If the operation is multiplication, the inverse of 'a' is 'a^{-1}' and is defined as $aa^{-1} = a^{-1}a = 1.$

In addition to the above laws, a group may satisfy the commutative law; i.e. a+b = b+a, or if the operation is multiplication, ab = ba. Such a group is called an Abelian or a Commutative group.

2.1.2 Rings:

A ring R is a set of elements for which two operations

are defined. One is addition and the other multiplication, even though these may not be ordinary addition or multiplication of numbers. In order for $\underline{/}$ R to be a ring, the following rules must apply:

Rule 1: The set R is an abelian group under addition.

Rule 2: (Closure). For any two elements a and b of R, the product ab is defined and is an element of R.

Rule 3 (Associative Law): For any three elements a,b, and c of R, a(bc)=(ab)c.

Rule 4 (Distributive Law): For any three elements a,b and c of R, a(b+c)=ab+ac and (b+c)a=ba+ca.

A ring is called commutative if its multiplication operation is commutative, i.e. for any two elements a and b ab=ba.

2.1.3 Fields: A field is a commutative ring with an unit element (multiplicative identity) in which every non-zero element has a multiplicative inverse.

2.3 SUBGROUPS AND COSETS:

A subset of elements of a group G is called a subgroup H, if it satisfies all the rules for a group itself. H is a subgroup if it satisfies the rules for closure and the rule of inverse also applies. For a set which fulfils the two rules,the identity must also be present.

Suppose the elements of a group G are $g_1, g_2, g_3 \ldots$, and the elements of a subgroup H are $h_1, h_2, h_3 \ldots$, and consider the array formed as follows:

The first row is the subgroup, with the identity at the left and each other element appearing once and only once. The first element in the second row is any element not appearing in the first row, and the rest of the elements are obtained by operating on each subgroup element by this first element on the left. Similarly a third, fourth and fifth rows are formed each with a previously unused group element in the first column, until all the group elements appear somewhere in the array.

$$
\begin{aligned}
h_1 &= 1, & h_2 &, & h_3, & \cdots & , & h_n \\
g_1 h_1 &= g_1, & g_1 h_2 &, & g_1 h_3, & \cdots & , & g_1 h_n \\
g_2 h_1 &= g_2, & g_2 h_2 &, & g_2 h_3, & \cdots & , & g_2 h_n \\
& \vdots \\
g_m h_1 &= g_m, & g_m h_2 &, & g_m h_3, & \cdots & , & g_m h_n
\end{aligned}
$$

The set of elements in a row of this array is called a left coset and the element appearing in the first column is called the coset leader. Right cosets could be similarly formed. Also every element of the group G is in one and only one coset of a subgroup H.

2.3 GALOIS FIELDS:

Before defining the Galois fields, associated termi-
nologies are explained.

2.3.1 Ideals, Residue Class and Residue Class Rings:

An ideal I is a subset of elements of a ring R with
the properties that I is a subgroup of the additive group of
R and for any element 'a' of I and any element 'r' of R, ar
and ra are in I. Since an ideal is a subgroup, cosets can be
formed. In this case the cosets are called residue classes
and all properties of cosets apply to residue classes also.
The residue classes of a ring with respect to an ideal forms
a ring and this ring is called the residue class ring.

2.3.2 Ground Fields, Extension Fields:

The residue class ring modulo m is a field if and only
if m is a prime number. These fields are called prime fields,
or Galois fields of p elements, GF(p).

If $r(x)$, $s(x)$ and $t(x)$ are polynomials and $r(x)$ $s(x) =$
$t(x)$, then it is said that $t(x)$ is divisible by $r(x)$ or that
$r(x)$ divides $t(x)$, and that $r(x)$ is a factor of $t(x)$. A
polynomial $p(x)$ of degree n which is not divisible by any
polynomial of degrees less than n but greater than 0 is
called irreducible.

Let $p(x)$ be the polynomial with coefficients in a field F. If $p(x)$ is irreducible in F, that is, if $p(x)$ has no factors with coefficients in F, then the algebra of polynomials over F modulo $p(x)$ is a field. The field formed by taking polynomials over a field F modulo an irreducible polynomial $p(x)$ of degree k is called an extension field of degree k over F. The original field F is called the ground field.

2.4 GENERALISED INVERSES OF MATRICES:

The concept of division does not exist in matrix algebra, however, an equivalent operation results when the matrix is multiplied by an unique matrix, called an 'inverse' to obtain the identity matrix, the 'one' of matrix algebra. The idea of inverse is that if $Ax = b$ then $x = A^{-1}b$ and this A^{-1} is such that $A^{-1}A = I$. This A^{-1} exists only if matrix A is non-singular and is a square matrix.

This unique inverse is at times denoted as M also, as this matrix M satisfies the four conditions given by Moore and Penrose and hence at times it is also known as the Moore-Penrose inverse. The four conditions are,

    i) $AMA = A$

    ii) $MAM = M$

    iii) AM is symmetric and

    iv) MA is symmetric.

The matrix M defined by the four Moore-Penrose conditions is unique for a given A. But there are many matrices G which satisfy just the first Moore-Penrose condition.

$$AGA = A$$

Any matrix G that satisfies this condition is called a generalised inverse of A, for A of dimension pxq and G of dimension qxp. Thus many matrices G may be found that satisfy this condition, the one exception is when A is non-singular in which case there is only one G and it is the regular inverse $G = A^{-1} = M$. The matrix G has numerous other names, depending on the various number of conditions it satisfies. The M inverse of A is denoted by A^{-1} and the generalised inverse by A^{-}.

2.4.1 An Algorithm to Find the Generalised Inverse G:

Matrix A has dimension p x q and A_{11} is the leading sub-matrix and is non-singular of rank r_A. Then a generalised inverse may be obtained as

$$A_{p \times q} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \quad \text{is } G_{q \times p} = \begin{bmatrix} A_{11}^{-1} & 0 \\ 0 & 0 \end{bmatrix}$$

where the null matrices in G have appropriate order to make

G q x p, the verification of $AGA = A$ involves using

$$A_{22} = A_{21} \, A_{11}^{-1} \, A_{12}.$$

However if A_{11} is not a non-singular sub-matrix of order r, then by elementary operations on the matrix a non-singular submatrix of order r may be brought to the leading position and then by partitioning the matrix B, and applying the same elementary operation on the generalised inverse so obtained, the generalised inverse G of matrix A may be obtained. Let R and S be the permutation matrices such that RAS brings a non-singular matrix of rank r_A to the leading position. Thus

$$RAS = B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

then F, the generalised inverse of B is $F = \begin{bmatrix} B_{11}^{-1} & 0 \\ 0 & 0 \end{bmatrix}$

and therefore G = SFR, which is a generalised inverse of A.

2.5 DIRECT PRODUCT OF MATRICES:

The direct product of two matrices $A_{p \times q}$ and $B_{m \times n}$ may be defined as

$$A_{pxq} \otimes B_{mxn} = \begin{bmatrix} a_{11}B & \cdots & a_{1q}B \\ \vdots & & \\ a_{p1}B & \cdots & a_{pq}B \end{bmatrix}$$

and is called as Kronecker product or Zehfuss product.
The product matrix is partitioned into as many submatrices
as there are elements of A, each submatrix being B multi-
plied by an element of A. Therefore the elements of the
direct product consist of all possible products of ⋅ elements
of A multiplied by an element of B. It has, in general,
order pm x qn.

Direct product, therefore, is an unique manner of
factorising a matrix defining a transformation and hence
implementation of the transformation can be accomplished
with reduced number of arithmetic operations.

Some useful results of direct product of matrices are

a) $R_{\langle ij \rangle} = R_{\langle i_0 i_1 i_2 \rangle \langle j_0 j_1 j_2 \rangle} = a_{i_0 j_0} \; b_{i_1 j_1} \; c_{i_2 j_2} \cdots$

where $R = A \otimes B \otimes C \cdots$ and i_i, j_i are mixed radices.

b) If a_{11} and a_{21} are the eigen-values of A a matrix and
b_{11} and b_{21} and so on of the others then the eigen-values
of the resultant matrix $A \otimes B \otimes \cdots$ is the product of their
individual eigen-values.

i.e. $a_{11} b_{11}$, $a_{11} b_{21}$, $a_{21} b_{11}$ and $a_{21} b_{21}$ and so on.

c) If a_{11} , b_{11} $\cdots$ are simple roots of the characteristic
   a_{21} b_{21}

equation of the matrices A and B, then the eigen-vectors of

of $C = A \otimes B$ are $a_{11}b_{11}$ and so on.

$$a_{11}b_{21}$$
$$a_{21}b_{11}$$
$$a_{21}b_{21}$$

2.6 EIGENVALUES AND EIGENVECTORS OF MATRICES:

For u a vector and γ a scalar, the equation

$$Au = \gamma u$$

may be valid for a given matrix A. The conditions for which this equation is valid, other than for $u = 0$, is that $A-\gamma I$ is singular i.e. $|A-\gamma I| = 0$. The above condition may be rewritten as

$$(A - \gamma I) u = 0$$

A non-null solution for u may be obtained as

$$u = [(A - \gamma I)^{-} \cdot (A-\gamma I)-I]z$$

using a generalised inverse of $(A-\gamma I)$ and where z is arbitrary.

The condition $|A-\gamma I| = 0$ is called the characteristic equation of A. For A of order n, the characteristic equation is a polynomial equation in γ of order n, with n roots denoted by $\gamma_1, \gamma_2, \ldots \gamma_n$, some of which may be the same and some of which may be zero. These roots are called latent-roots, characteristic-roots, proper roots, eigenvalues or γ-roots. Corresponding to each γ_i is a vector u_i which satisfies

A $u_i = \gamma_i u_i$ for i=1,...n and these vectors $u_1, u_2, \ldots u_n$ are correspondingly called latent-vectors, characteristic-vector proper-vector or eigenvector. And the matrix $[A-\gamma I]$ is called the characteristic matrix.

The set of all vectors u, which form the columns of a matrix is called as a model matrix. Model matrix may also be found using Jordan canonical matrix [12].

2.6.1 Calculating Eigenvectors:

Supposing γ_k is an eigenvalue of A. It is a solution of the characteristic equation $|A-\gamma I| = 0$. Determining an eigenvector corresponding to γ_k implies finding a non-null u to satisfy $Au = \gamma_k u$, which is equivalent to solving

$$(A - \gamma_k I)u = 0$$

The number of linearly independent solution to the above equation are $n-r(A-\gamma_k I)$ i.e. the order of the matrix minus the rank of the characteristic matrix (corresponding to the characteristic value) and these solutions are

$$u_k = [(A-\gamma_k I)^- (A-\gamma_k I)-I]z \quad \text{and}$$

since γ_k is such that $|A-\gamma_k I| = 0$; $A-\gamma_k I$ is singular and so at least one non-null solution always exists. For each γ_k, the characteristic matrix $[A-\gamma_k I]$ is processed by elementary operations and a matrix B_k is obtained to enable partition the matrix as,

$$B_k = \begin{bmatrix} R_k & C_k \\ D & E \end{bmatrix}$$

such that the submatrix R_k is non-singular with the same rank as the characteristic matrix $[A-\gamma_k I]$ and then obtain the generalised inverse of the characteristic matrix as

$$(A-\gamma_k I)^- = \begin{bmatrix} R_k^{-1} & O \\ O & O \end{bmatrix}$$

and so obtain the solution

$$u_k = \begin{bmatrix} -R_k^{-1} C_k w \\ w \end{bmatrix} \quad \text{for arbitrary } w \text{ of order}$$

$n-r(A-\gamma_k I)$.

2.6.2 Simple and Multiple Roots:

A number of eigen-vectors u_k are found from the general solution for each eigenvalue γ_k of the matrix including $\gamma_k=0$, if it occurs. Since γ_k is a solution to the characteristic equation it may be a solution more than once, in which case it is called a multiple root. If γ_k is a solution only once it is called as a simple root. When γ_k is a simple root the rank of the characteristic matrix $r(A-\gamma_k I) = n-1$. Therefore there is just only one LIN eigen-vector corresponding to γ_k. This is reflected in w as w

becomes a scalar. When γ_k is a solution more than once it is called as multiple roots and the number of times that it is a solution is called its multiplicity. For each multiple eigenvalue γ_k, with multiplicity m_k, the rank of $A-\gamma_k I$ must be ascertained as this is the value that plays an important role in the determination of eigen-vectors.

2.7 NULL-SPACE AND DIMENSION OF NULL-SPACE OF MATRICES:

In Sec. 1.1, the linear transformation was identified with an n x n matrix R. T was the linear transformation of a vector space C into a vector space A. The null-space of a linear transformation T is the set of all vectors such that $c_i^T = 0$, and the null-space of a matrix R is the set of all row matrices X which satisfy the homogenous linear equation XR = 0. Alternatively, the null-space of the row space of a matrix is called the null-space of the matrix. A vector is in the null-space of a matrix if it is orthogonal to each row of the matrix. The dimension of the null-space of a given matrix is called as **nullity** of the matrix. The rank and nullity of an n x n matrix is related by the following equation.

Order of the matrix - rank of thematrix = nullity.

CHAPTER 3

EIGEN-STRUCTURE OF REED-MULLER MATRICES

Methods to obtain the positive canonic RM expansion coefficients from the minterm coefficients (obtained from the truth-table entries of a Boolean function) have been developed [7],[10],[21],[22],[23]. In the methods developed in [7],[10] other non-positive canonic RM expansion coefficients have been obtained from the positive canonic RM expansion coefficients. In the geometric mapping method [7], the map folding operations become difficult when the number of variables in the Boolean function increases. Moreover, if this difficulty is surmounted then in any map method there is no freedom to represent the variables than the available 3 dimensions, with utmost four variables represented in each dimension. The limitations of the b_j maps have been overcome in the computer method [10].

In this chapter the RM matrix structures, for different polarity functions have been obtained as a direct-product of two kinds of core matrices. Techniques have also been developed, or suitably adopted, to determine the eigen-structure.

3.1 RM MATRICES:

In Chapter 1 the method of obtaining any non-positive canonic RM expansion from any other expansions by algebraic

substitutions and simplification [24] was illustrated by
(1.8), (1.9), (1.10) and (1.11). For this example   the
transformation, in the matrix form would be

$$R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

This is the transformation from the minterm coefficients,
obtained from the truth-table entries of the Boolean function,
to the non-positive canonic RM expansion coefficients. This
particular transformation pertains to the polarity function
110 of the 3 variable Boolean function. The RM matrix, for
the positive canonic RM expansion, was also obtained iteratively
(1.14) which may also be obtained as direct product of, what
has been termed as the core matrix, for m' = 0 in (1.14), i.e.
the 2x2 matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. To obtain the RM matrix, for the
non-positive canonic RM expansions, suitable core matrix,
to be called as core matrix for a complemented variable,
would have to be appropriately multiplied with the other core

matrices; by multiplication is meant the direct product
as per some rules.

The eigen-values and eigen-vectors of the Reed-Muller
matrices help in obtaining the positive canonic and non-
positive canonic expansion coefficients and therefore, the
eigen-structure of the RM matrices have been developed in
this chapter subsequently. The results obtained in this
chapter have been used in the next chapter, in which tne
algorithms to obtain the expansion coefficients have been
developed. As the Reed-Muller matrices have been developed
as direct product of the core matrices, the eigen-values
too have been obtained as direct product of the eigen-values
of the core matrices. As brought out earlier the eigen-vectors
for repetitive roots (eigen-values) of the characteristic
matrix of RM matrices, have to be uniquely obtained by
employing the generalised inverses of the characteristic
matrix or using the concept of null-space of the characteristic
matrix.

3.2 THE CORE MATRICES:

In the previous section the core matrix for the
'positive' variable was identified. Like the RM matrix,
for the positive canonic RM expansion, this core matrix is also
involutary, i.e. the matrix is its own inverse. Similarly

to obtain the RM matrices, for non-positive canonic RM

expansions, a core matrix to represent the complemented

variable is identified as that matrix which results when

the core matrix for a positive variable is multipled by the

counter identity matrix J. This is represented as

$$B_{\bar{x}} = B_x \cdot J = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \qquad 1)$$

and may be called as the core matrix for a complemented

variable.

The characteristic equations of the two core matrices

are respectively,

$$(\gamma + 1)^2 = 0 \qquad (3.2.2)$$

$$(\gamma^2 + \gamma + 1) = 0 \qquad (3.2.3)$$

The roots of the characteristic equation of the core matrix

is $\gamma=1$ and $\gamma=1$. The repetition of a root is also termed as

its multiplicity and is denoted by m_k. Therefore the

characteristic roots of the core matrix may be written as

$\gamma=1$, $m_1=2$. The characteristic equation of the core matrix

for a complemented variable is an irreducible polynomial of

degree 2. Therefore, the roots are not in the ground field,

GF(2) and are to be found in the first extension field viz.

$(GF2^2)$ and the roots would be from the elements of the

extension field, viz. $0,1,\alpha$ and $1+\alpha$, with $\alpha^2+\alpha+1 = 0$ being the irreducible polynomial. Hence, the characteristic roots of the core matrix of a complemented variable are $\gamma=\alpha$ and $\gamma=1+\alpha$, with multiplicity one each. It is also observed that the irreducible polynomial is of degree 2 and therefore the characteristic roots always occur as a set.

3.3 OBTAINING RM MATRICES AS DIRECT-PRODUCT OF CORE MATRICES:

A given m variable Boolean function may be associated to the corresponding RM expansion coefficients through transforms, called as the RM matrices. It was also described in Chapter 1, that the RM matrices may be classified as the RM matrix for the positive canonic RM expansion or the CFRM expansion and as the RM matrices that represent the other non-positive canonic RM expansions, called as the generalised Reed-Muller expansions. In this section, the method for obtaining the two kinds of Reed-Muller matrices, as direct-product of the two kinds of core matrices, is developed.

3.3.1 RM Matrix for Positive Canonic RM Expansion:

The RM matrix for the positive-canonic RM expansion, in which all the m variables of the Boolean function are in the positive form, is obtained as direct product of the core matrices. The m variable Boolean function is said to

have all positive polarity function and hence each of the

m variable of the Boolean function is represented by a core

matrix. Therefore, the Reed-Muller matrix, so obtained

is of order n, $n=2^m$. For the Boolean function of m variables,

this may be written as

$$R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \cdots (\otimes) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ m times} \qquad (3.3.1)$$

The RM matrix so obtained is also involutary.

3.3.2 RM Matrix for Non-positive Canonic RM Expansions:

In the non-positive canonic expansion, one or more

variables of the Boolean function appear in the complemented

form, but the same variable does not appear in both the forms

in the expansion. The RM matrix corresponding to these

expansions would, therefore, be dependent on the polarity

function of the Boolean function and is obtained as direct-

product of both kinds of core matrices. Each variable in the

function which has positive polarity is represented by the

core matrix and the variable that is complemented by the core

matrix of a complemented variable. For the Boolean function

of m variables, which has the polarity function 1101001...1,

the RM matrix is obtained as direct product of the appropriate

core matrices in that order.

$$R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\otimes \cdots \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ m times} \qquad (3.3.2)$$

Therefore, if there are t variables complemented in the m variable functions, there are (m-t) core matrices and t core matrices, for a complemented variable. The RM matrices so obtained is unlike the RM matrix for the positive canonic RM expansions, i.e. is not involutary. Here too the order of the RM matrix is n, $n=2^m$.

3.4 GOOD'S FACTORISATION OF RM MATRICES:

The RM matrices have a high degree of redundency and if the redundency in the definition of the matrix transformation is eliminated by matrix factorisation then a more efficient means of implementation is possible. Such a technique was employed in the development of the fast Fourier transform (FFT) and fast Hadamard transform (FHT) and to a large class of fast transformations [14].

A class of matrices formed by Kronecker product operation may be considered as the square submatrices of order p, with entries $m_{r,i,j}$, where i and j range from O to p-1, and the first index r representing the class of entries corresponding to a particular dimension in the Kronecker product operation. In general

$$M_r = \begin{bmatrix} m_{r,0,0} & m_{r,0,1} & \cdots & m_{r,0,p-1} \\ m_{r,1,0} & m_{r,1,1} & \cdots & m_{r,1,p-1} \\ \vdots & & & \\ m_{r,p-1,0} & m_{r,p-1,1} & \cdots & m_{r,p-1,p-1} \end{bmatrix} \qquad (3.4.1)$$

and

$$(3.4.2)$$

$$H_1 = M_0$$

$$H_2 = M_1 \otimes H_1$$

$$\vdots$$

$$H_q = M_{q-1} \otimes H_{q-1}$$

Thus

$$H_q = \begin{bmatrix} m_{q-1,0,0} \, H_{q-1} & \cdots & m_{q-1,0,p-1} \, H_{q-1} \\ m_{q-1,1,0} \, H_{q-1} & \cdots & m_{q-1,1,p-1} \, H_{q-1} \\ \vdots & & \\ m_{q-1,p-1,0} H_{q-1} & \cdots & m_{q-1,p-1,p-1} \, H_{q-1} \end{bmatrix} \qquad (3.4.3)$$

where

$$H_q \text{ is a } p^q \otimes p^q \text{ matrix}$$

When operating with Kronecker matrices within a computer, it becomes desirable to store a representation (algorithm) of the entries of the product matrix rather than

the matrix itself. The location in the matrix may be described by their lexicographic sequence representation. A given index of matrix H_q may thus be represented by q digits each of which may take the value 0 to p-1. Representing the horizontal index by v and the vertical index by x, the names of the rows and columns in lexicographic sequence for H_2 matrix for p=3 is

$$
\begin{array}{c}
v \longrightarrow \\
\text{00 01 02 10 11 12 20 21 22}
\end{array}
$$

$$
x \downarrow \quad H_2 = \begin{array}{c} 00 \\ 01 \\ 02 \\ 10 \\ 11 \\ 12 \\ 20 \\ 21 \\ 22 \end{array}
\left[\quad H_2(x,v) \quad \right]
$$

$$(3.4.4)$$

Representing the v and x variables in the lexicographic number system, modulo p, requires q digits to allow v and x to range over 0 to p^q. Therefore v and x may be described by

$$v = v_{n-1} \; v_{n-2} \cdots v_1 v_0 \quad v_i \quad 0,1,\ldots,p-1 \qquad (3.4.5)$$

$$x = x_{n-1} \; x_{n-2} \cdots x_1 x_0 \quad x_i \quad 0,1,\ldots,p-1$$

Using such notation allows the entries of the p x p matrix H_1 (3.4.2) to be described by the equation

$$H_1(x,v) = \prod_{i=0}^{p-1} \prod_{j=0}^{p-1} m_{0,i,j}^{\partial(x_0-i)\partial(v_0-j)} \qquad (3.4.6)$$

where $\partial(a-b)$ is the delta function which takes on the value 1 whenever a=b and 0 otherwise. The representation of (3.4.6) may be interpreted as multiplying all entries of the core matrix, M_0 (3.4.2), together and noting that all but one entry would be raised to the 0th power. The entries of the p^2 by p^2 matrix, H_2, (3.4.4) may now be represented as

$$H_2(x,v) =$$

$$\prod_{i=0}^{p-1} \prod_{j=0}^{p-1} m_{1,i,j}^{\partial(x_1-i)(v_1-j)} \quad \prod_{i=0}^{p-1} \prod_{j=0}^{p-1} m_{0,i,j}^{\partial(x_0-i)\partial(v_0-j)}$$

$$(3.4.7)$$

where the exponents determine the correct product of entries for a given v and x. In general, the entries for H_q may be represented as,

$$H_q(x,v) = \prod_{r=0}^{q-1} \prod_{i=0}^{p-1} \prod_{j=0}^{p-1} m_{r,i,j}^{\partial(x_r-i)\partial(v_r-j)} \qquad (3.4.8)$$

following the recursive notation of (3.4.6) and (3.4.7). Representation of the rows or columns of a Kronecker matrix in the form of (3.4.8) allows the generation of any single

element, column or row of the matrix without storage of the
entire matrix array. The operation indicated in (3.4.8)
may be visualised as multiplying all entries of the sub-
matrices, M_r, forming the Kronecker Product, together and
letting the exponent operation allow only the proper entries to
be raised to power 1 while all others are raised to the power
0. For the Kronecker product of identical matrices

$$H_q(x,v) = \prod_{i=0}^{p-1} \prod_{j=0}^{p-1} m_{i,j}^{\sum_{r=0}^{n-1} \delta(x_r-1)\delta(v_r-j)} \qquad (3.4.9)$$

A major observation was made about the matrix facto-
risation i.e. if highly redundant matrices could be factored
into a product of matrices with few non-zero entries, then a
fewer number of operations would be necessary for transfor-
mation implementation. A technique, attributable to Good
[26], of matrix factorisation, may be used to decompose the
class of Kronecker matrices described by (3.4.8) or (3.4.9).
Thus for the H_q Kronecker matrix of (3.4.8), there exists q
matrices, each of dimension p^q, such that when multiplied
together will equal H_q. These matrices may be described as

42

$$G_r = \begin{bmatrix} m_{r,o,o}\cdots m_{r,o,p-1} & & & \\ & m_{r,o,o}\cdots m_{r,o,p-1} & & \\ & & \vdots & \\ & & & m_{r,o,o}\cdots m_{r,o,p-1} \\ m_{r,o,o}\cdots m_{r,1,p-1} & & & \\ & m_{r,o,o}\cdots m_{r,1,p-1} & & \\ & & \vdots & \\ & & & m_{r,1,o}\cdots m_{r,1,p-1} \\ \cdots & \cdots & \cdots & \\ m_{r,p-1,o}\cdots m_{r,p-1,p-1} & & & \\ & m_{r,p-1,o}\cdots m_{r,p-1,p-1} & & \\ & & \vdots & \\ & & & m_{r,p-1,o}\cdots m_{r,p-1,p-1} \end{bmatrix}$$

(3.4.10)

In this matrix there are p^{q+1} non-zero entries and only p^2 non-redundant elements. Then

$$H_n = [G_{n-1}][G_{n-2}]\ldots[G][G_0] \qquad (3.4.11)$$

and for the Krocker product of identical matrices

$$H_n = [G]^n \qquad (3.4.12)$$

The RM matrices obtained earlier (3.3.1) and (3.3.2) may be factorised respectively as,

where,

$$R_x = \begin{bmatrix} 10 & & & & \\ & 10 & & & \\ & & 10 & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & 10 \\ 11 & & & & \\ & 11 & & & \\ & & 11 & & \\ & & & 11 & \\ & & & \cdot & \\ & & & & 11 \end{bmatrix} \begin{array}{l} \\ n/2 \text{ rows} \\ \\ \\ \\ \\ \\ n/2 \text{ rows} \end{array}$$

n columns

$$(3.4.14)$$

and,

$$R = \begin{bmatrix} 10 & & & \\ 11 & & & \\ & 10 & & \\ & 11 & & \\ & & 10 & \\ & & 11 & \\ & & \cdot & \\ & & & 10 \\ & & & 11 \end{bmatrix}^2 \begin{bmatrix} 01 & & & \\ 11 & & & \\ & 01 & & \\ & 11 & & \\ & & 01 & \\ & & 11 & \\ & & \cdot & \\ & & & 01 \\ & & & 11 \end{bmatrix} \begin{bmatrix} 10 & & & \\ 11 & & & \\ & 10 & & \\ & 11 & & \\ & & 10 & \\ & & 11 & \\ & & \cdot & \\ & & & 10 \\ & & & 11 \end{bmatrix}^2 \begin{array}{l} \\ \\ \cdots \text{ as per} \\ \text{the} \\ \text{polarity} \\ \textbf{function} \end{array}$$

$$(3.4.15)$$

$$= R_x \; R_x \; \cdot \; R_x \; R_x \; R_x \; \cdots \; m \text{ times}$$

where $R_{\dot{x}} = R_x$ and $R_{\ddot{x}} = R_{\bar{x}}$ as per the polarity function, and

$$
R_{\bar{x}} = \begin{bmatrix}
01 & & & & \\
& 01 & & & \\
& & 01 & & \\
& & & \ddots & \\
& & & & 01 \\
11 & & & & \\
& 11 & & & \\
& & 11 & & \\
& & & \ddots & \\
& & & & 11
\end{bmatrix}
\quad
\begin{matrix}
n/2 \text{ rows} \\
\\
\\
\\
n/2 \text{ rows}
\end{matrix}
\qquad (3.4.16)
$$

both R_x and $R_{\bar{x}}$ obtained by ~~rearranging the rows of~~ (3.4.10).

3.5 EIGENVALUES OF THE REED-MULLER MATRICES:

The eigenvalues or the characteristic roots of a
matrix   are the solutions to the equation,

$$Ru = \gamma u \qquad (3.5.1)$$

for R a matrix and u, a vector and γ, a scalar. There are
a number of scalars and vectors that satisfies this equation;
the scalars are called as eigenvalues and the set of eigen-
values is are termed as the spectrum of R. The eigenvalues
are also obtained by solving thecharacteristic equation

$$(R - \gamma I) = 0 \qquad (3.5.2)$$

In the previous section the RM matrices were obtained as direct-
product of the core matrices and were classified as RM matrix

for the positive canonic RM expansion and RM matrices for the non-positive canonic RM expansion. The polarity function of the variables of the Boolean function determines the kinds of roots and their multiplicity. In this section the eigenvalues are not found as solutions to the characteristic matrices of the RM matrices (3.5.2) but the property of direct-product is exploited.

3.5.1 Eigen-value of the RM Matrix, for Positive Canonic RM expansion:

The RM matrix for the CFRM expansion was obtained as direct product of the core matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ (3.3.1); the order of the matrix being $n=2^m$. Therefore there are utmost 2^m eigenvalues. The eigenvalues of the core matrix are $\gamma=1$, with multiplicity $m_1=2$ and therefore, the eigenvalues of the RM matrix for the CFRM expansion are $\gamma=1$, $m_1=n$. And, therefore may be written as

$$\text{Spectrum of } R = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \cdots \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad , \quad \gamma=1, m_1=2^m \quad (3.5.3)$$

3.5.2 Eigen-values of RM Matrices, for Non-positive Canonic RM expansions:

The eigenvalues of the RM matrices, for the non-positive canonic RM expansion may be obtained as the direct product of the eigenvalues of the core matrices. The characteristic equation of the core matrix for a complemented variables being

an irreducible polynomial of degree 2, the roots are found
in the extension field only and the roots occur as a set
viz. $\gamma = \alpha$ and $\cdot = 1 + \alpha$. The number of eigenvalues of the RM
matrices is dependent on the polarity function i.e. on the
number of variables of the function and the number of
variables complemented. Hence, the number of eigen-values
of two RM matrices may be the same but the pattern of the
polarity function being different, their eigenvectors would
be different.

For the polarity functions in which there is only one
variable complemented, all roots of the characteristic
equations for the RM matrices are to be found in the extension
field alone. This is unique only to the case mentioned,
because irrespective of the number of variables, if there is
only one variable complemented of these, then the eigen-values
of the core matrix of a complemented variable manifests
the entire operations of the direct product and therefore
the roots are found only in the extension field.

In general it may be written as

$$R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \cdots \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad m \quad \text{times}$$

Spectrum of R =

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \cdots \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad m \quad \text{times}$$

$$= \begin{bmatrix} 1(2^{m-2}) \\ 1(2^{m-2}) \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix}$$

$$= \begin{bmatrix} \alpha \ (2^{m-1}) \\ 1+\alpha(2^{m-1}) \end{bmatrix}$$

i.e. $\gamma = \alpha$, $m_\alpha = 2^{m-1}$

$\gamma = 1+\alpha$, $m_{1+\alpha} = 2^{m-1}$

Cases where more than one variable occurs complemented the eigenvalues $\gamma=1$, $\gamma=\alpha$ and $\gamma=1+\alpha$ are obtained and satisfy the condition

$$m_1 + m_\alpha + m_{1+\alpha} = 2^m \qquad (3.5.4)$$

as utmost 2^m eigenvalues may be had for the RM matrix of order $n, n=2^m$. As a result of the polarity function, the first three variables in this category may occur as

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} = \begin{bmatrix} 1(4) \\ \alpha(2) \\ 1+\alpha(2) \end{bmatrix}$$

$$\text{or} \quad \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1(4) \\ \alpha(2) \\ 1+\alpha(2) \end{bmatrix}$$

$$\text{or} \quad \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} = \begin{bmatrix} 1(4) \\ \alpha(2) \\ 1+\alpha(2) \end{bmatrix}$$

(for ease, the multiplicity is being indicated in parenthesis).

Now the variables following may be true or complemented, and
would occur as per the polarity functions. If the variable is
true then

$$\begin{bmatrix} 1(4) \\ \alpha(2) \\ 1+\alpha(2) \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1(8) \\ \alpha(4) \\ 1+\alpha(4) \end{bmatrix} \qquad (3.5.5)$$

i.e. $m_1' = 2.m_1$, $m_\alpha' = 2.m_\alpha$ and $m_{1+\alpha}' = 2.m_{1+\alpha}$

(where the prime on the multiplicity indicates the multiplicity
after the direct product operation) and if the variable is
complemented, then

$$\begin{bmatrix} 1(4) \\ \alpha(2) \\ 1+\alpha(2) \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} = \begin{bmatrix} 1(4) \\ \alpha(6) \\ 1+\alpha(6) \end{bmatrix} \qquad (3.5.6)$$

i.e. $m_1' = m_\alpha + m_{1+\alpha}$, $m_\alpha' = m_1 + m_\alpha$, $m_{1+\alpha}' = m_1 + m_{1+\alpha}$

It was observed that the eigenvalues, though a function
of the polarity function, depended more on the number of
variables complemented; the odd number of complemented variables
demonstrating a common feature amongst them and the even
number of complemented variables demonstrating another
common feature amongst them.

Starting with two complemented variables, the resulting
eigenvalues would be

$$[_{1+\alpha}^{\alpha}] \otimes [_{1+\alpha}^{\alpha}] = \begin{bmatrix} 1(2) \\ \alpha(1) \\ 1+\alpha(1) \end{bmatrix} \qquad (3.5.7)$$

then with other complemented variables following this, the rule given in (3.4.6)could be applied. It was observed that when even number of variables are complemented $m_1 = m_\alpha + 1 = m_{1+\alpha} + 1$ and when odd number of variables are complemented then $m_1 = m_\alpha - 1 = m_{1+\alpha} - 1$, which results as an outcome of the operation over the irreducible polynomial $\gamma^2 + \gamma + 1 = 0$. The eigenvalues of ten complemented variables are considered before generalisation.

The eigenvalues of t complemented variables, obtained as a direct product of the eigenvalues of the core matrices for complemented variables, is tabulated to illustrate the observation that the eigenvalues are indeed a factor of t being odd or even and that the rules

$$m_1 = m_\alpha + 1 = m_{1+\alpha} + 1 \text{ (for t even)}$$

and $\quad m_1 = m_\alpha - 1 = m_{1+1} - 1$ (for t odd) holds.

The table shows the multiplicity of each root.

Table 3.5.1

No. of variables	1	2	3	4	5	6	7	8	9	10	
The eigenvalues	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	α $1+\alpha$	
1	-	2	2	6	10	22	42	86	170	342	
α	1	1	3	5	11	21	43	85	171	341	
'1+α'	1	1	3	5	11	21	43	85	171	341	

Now generalising (3.5.6), two sets of formulae one each for t odd and t even may be written as

1) t odd:

$$\gamma = 1 \quad m_1 = \frac{2^t - 2}{3} \qquad (3.5.8)$$

$$\gamma = \alpha \quad m_\alpha = \frac{2^{t+1} + 2}{6}$$

$$\gamma = 1+\alpha \quad m_{1+\alpha} = \frac{2^{t+1} + 2}{6}$$

ii) t even:

$$\gamma = 1 \quad m_1 = \frac{2^t + 2}{3} \qquad (3.5.9)$$

$$\gamma = \alpha \quad m_\alpha = \frac{2^{t+1} + 2}{6}$$

$$\gamma = 1+\alpha \quad m_{1+\alpha} = \frac{2^{t+1} - 2}{6}$$

If $t = m$, i.e. all variables are complemented then the condition (3.4.4) must also hold i.e.

$$m_1 + m_\alpha + m_{1+\alpha} = \frac{2^t - 2}{3} + \frac{2^{t+1} + 2}{6} + \frac{2^{t+1} + 2}{6} = 2^t = 2^m$$

$$= \frac{2^t + 2}{3} + \frac{2^{t+1} - 2}{6} + \frac{2^{t+1} - 2}{6} = 2^t = 2^m$$

Now if these t variables were complemented out of the total m variables of the function, the remaining $(m-t)$ variables being true, the eigenvalues of the RM matrices is obtained by multiplying the eigenvalues obtained for t variables by a factor of $2^{(m-t)}$ Eqn. (3.5.3) refers. Therefore the multiplicity of the eigenvalues of RM matrices for an m variable function, with t variables complemented as a function of m and t are obtained as

i) t odd:

$$\gamma = 1 \quad m_1 = 2^{(m-t)} \quad \frac{2^t - 2}{3} \tag{3.5.10}$$

$$\gamma' = \alpha \quad m_\alpha = 2^{(m-t)} \quad \frac{2^{t+1} + 2}{6}$$

$$\gamma = 1+\alpha \quad m_{1+\alpha} = 2^{(m-t)} \quad \frac{2^{t+1} + 2}{6}$$

ii) t even:

$$\gamma = 1 \quad m_1 = 2^{(m-1)} \quad \frac{2^t + 2}{3} \tag{3.5.11}$$

$$\gamma = \alpha \qquad m_\alpha = 2^{(m-t)} \quad \frac{2^{t+1}+2}{6}$$

$$\gamma = 1+\alpha \quad m_{1+\alpha} = 2^{(m-t)} \quad \frac{2^{t+1}+2}{6}$$

and these sets of formulae also satisfy the condition (3.5.4) $m_1 + m_\alpha + m_{1+\alpha} = 2^m$, i.e.

i.e., $2^{(m-t)} \left(\frac{2^t-2}{3} + \frac{2^{t+1}+2}{6} + \frac{2^{t+1}+2}{6} \right) = 2^m$

and $2^{(m+t)} \left(\frac{2^t+2}{3} + \frac{2^{t+1}-2}{6} + \frac{2^{t+1}-2}{6} \right) = 2^m.$

Illustrative Example 3.5.1

The number of variable m = 3

with polarity $x_3 \bar{x}_2 x_1$

The corresponding Reed Muller matrix $R = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 01 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 10 \\ 11 \end{bmatrix}$

$$R = \begin{bmatrix}
00 & 10 & 00 & 00 \\
00 & 11 & 00 & 00 \\
10 & 10 & 00 & 00 \\
11 & 11 & 00 & 00 \\
00 & 10 & 00 & 10 \\
00 & 11 & C0 & 11 \\
10 & 10 & 10 & 10 \\
11 & 11 & 11 & 11
\end{bmatrix}$$

the eigenvalues are obtained as a direct product of

$\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}$ (x) $\begin{smallmatrix} \alpha \\ 1+\alpha \end{smallmatrix}$ (x) $\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}$ and the spectrum of R is $(\alpha, \alpha, 1+\alpha, 1+\alpha, \alpha, \alpha,$ $1+\alpha, 1+\alpha)$.

For the same number of variables if the polarity now is made as $\bar{x}_3 x_2 x_1$

the   Reed Muller matrix $R = \begin{bmatrix} 01 \\ 11 \end{bmatrix}$ (x) $\begin{bmatrix} 10 \\ 11 \end{bmatrix}$ (x) $\begin{bmatrix} 10 \\ 11 \end{bmatrix}$

$$R = \begin{bmatrix} 00 & 00 & 10 & 00 \\ 00 & 00 & 11 & 00 \\ 00 & 00 & 10 & 10 \\ 00 & 00 & 11 & 11 \\ 10 & 00 & 10 & 00 \\ 11 & 00 & 11 & 00 \\ 10 & 10 & 10 & 10 \\ 11 & 11 & 11 & 11 \end{bmatrix}$$

The eigenvalues are obtained as $\begin{smallmatrix} \alpha \\ 1+\alpha \end{smallmatrix}$ (x) $\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}$ (x) $\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}$ a direct product and the spectrum of R is $(\alpha, \alpha, \alpha, \alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha)$.

It is thus seen that when there is only one variable being complemented, then all roots are in the extension field only and irrespective of the pattern of the polarity function, the eigenvalues are the same.

Illustrative Example 3.5.2:

Consider a 4 variable switching function

with polarity $x_4 x_3 x_2 \bar{x}_1$,

the corresponding Reed-Muller matrix $R = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 10 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 10 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 01 \\ 11 \end{bmatrix}$ a direct product

The eigenvalues are obtained as $\left(\begin{matrix} 1 \\ 1 \end{matrix} \otimes \begin{matrix} 1 \\ 1 \end{matrix} \otimes \begin{matrix} 1 \\ 1 \end{matrix} \otimes \begin{matrix} \alpha \\ 1+\alpha \end{matrix} \right)$ the spectrum of R being $(\alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha, \alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha)$ and for the same number of variables, with the polarities now assigned as $x_4 \bar{x}_3 x_2 x_1$.

The RM matrix becomes $R = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 01 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 10 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 10 \\ 11 \end{bmatrix}$

The eigenvalues are obtained as a direct product of

$$\begin{matrix} 1 \\ 1 \end{matrix} \otimes \begin{matrix} \alpha \\ 1+\alpha \end{matrix} \otimes \begin{matrix} 1 \\ 1 \end{matrix} \otimes \begin{matrix} 1 \\ 1 \end{matrix}$$

The spectrum of R being $(\alpha, \alpha, \alpha, \alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha, \alpha, \alpha, \alpha, \alpha, 1+\alpha, 1+\alpha, 1+\alpha, 1+\alpha)$.

It is once again observed that when there is only one variable being complemented, then all roots are in the extension field only and irrespective of the pattern of the polarity function, the eigenvalues are the same.

Hence for

$\quad m = 3, \ \gamma=\alpha, \ m_\alpha=4, \ $ and $ \ \gamma=1+\alpha, \ m_{1+\alpha}=4 \ $ and

$\quad m = 4, \ \gamma=\alpha, \ m_\alpha=8, \ $ and $ \ \gamma=1+\alpha, \ m_{1+\alpha}=8$.

Illustrative Example 3.5.3:

A 7 variable function with five variables complemented with the polarity function 1000 100 is considered.

The function is

$$(x_7, \tilde{x}_6, \tilde{x}_5, \bar{x}_4, x_3, \bar{x}_2, \bar{x}_1) \quad \text{and}$$

the eigenvalues are obtained as direct product of the eigenvalues of the core matrices as

$$[{}^1_1] \otimes [{}^{\alpha}_{1+\alpha}] \otimes [{}^{\alpha}_{1+\alpha}] \otimes [{}^{\alpha}_{1+\alpha}] \otimes [{}^1_1] \otimes [{}^{\alpha}_{1+\alpha}] \otimes [{}^{\alpha}_{1+\alpha}]$$

the number of eigenvalues after each direct-product operation	1(2)	$\alpha(2)$ $\alpha^2(2)$	1(4) $\alpha(2)$ $\alpha^2(2)$	1(4) $\alpha(6)$ $\alpha^2(6)$	1(8) $\alpha(12)$ $\alpha^2(12)$	1(24) $\alpha(20)$ $\alpha^2(20)$	1(40) $\alpha(44)$ $\alpha^2(44)$

and by formulae, t being odd

$$\text{for } \gamma = 1, \quad m_1 = 2^{(7-5)} \ \frac{2^5-2}{3} = 4 \cdot 10 = 40$$

$$\text{for } \gamma = \alpha, \quad m_\alpha = 2^{(7-5)} \ \frac{2^6+2}{3 \cdot 2} = 4 \cdot 11 = 44$$

$$\text{for } \gamma = 1+\alpha, \quad m_{1+\alpha} = 2^{(7-5)} \ \frac{2^6+2}{3 \cdot 2} = 4 \cdot 11 = 44.$$

Therefore $m_1 = 40$, $m_\alpha = 44$ and $m_{1+\alpha} = 44$ and $\Sigma \ m_i = 2^m$.

The same were obtained as direct product of eigenvalues of the core matrices also.

If for the same function the polarity is 1010100 then m=7, t=4.

for $\gamma=1$ $m_1 = 2^{(7-4)} \cdot \dfrac{2^4+2}{3} = 8.6 = 48$

for $\gamma=\alpha$ $m_\alpha = 2^{(7-4)} \cdot \dfrac{2^5-2}{3.2} = 8.5 = 40$

for $\gamma=1+\alpha$ $m_{1+\alpha} = 2^{(7-4)} \cdot \dfrac{2^5-2}{3.2} = 8.5 = 40$

and $\Sigma\, m_i = 2^m$

3.6 CHARACTERISTIC EQUATION:

The condition for a non-null solution to the equation (3.5.1)

$$Ru = \gamma u$$

for R, a matrix and u, a vector and γ, a scalar is that $R - \gamma I$ is singular i.e. $|R - \gamma I| = 0$. This condition is called as the characteristic equation of the matrix R. For the matrix R of order n, the equation is a polynomial equation in γ of degree n. The roots of this characteristic equations are called as the characteristic roots or the eigenvalue (Secs. 2.6. and 3.5 refer).

For the RM matrices, which are obtained as a direct-product of core matrices, the eigenvalues have also been obtained as direct product of the eigenvalues of the core matrices. These very eigenvalues being defined by the

characteristic equation, it is feasible to construct the characteristic equation from the eigenvalues. If $\gamma_1, \gamma_2 \cdots \gamma_k$ are the different eigenvalues with multiplicity $m_{\gamma_1}, m_{\gamma_2} \cdots m_{\gamma_k}$, then the characteristic equation may be written as

$$(\gamma-\gamma_1)^{m_{\gamma_1}} (\gamma-\gamma_2)^{m_{\gamma_2}} \cdots (\gamma-\gamma_k)^{m_{\gamma_k}} = 0 \qquad (3.6.1)$$

And in the case of RM matrices, whose roots are over the extension field $GF(2^2)$, with the irreducible polynomial $\gamma^2+\gamma+1 = 0$, and all operation being modulo 2, the equation may be written as

$$(\gamma+1)^{m_1} (\gamma^2+\gamma+1)^{m_\alpha} = (\gamma+1)^{m_1} (\gamma^2+\gamma+1)^{m_{1+\alpha}} = 0$$

$$(3.6.2)$$

and these equations may be specifically written for the m variables, of which t are complemented as

$$(\gamma+1)^{m_1} = 0 \quad \text{for } t = 0 \quad m_1 = 2^m$$

$$(\gamma^2+\gamma+1)^{m_\alpha} = 0 \quad \text{for } t = 1 \quad m_\alpha = 2^{m-1}$$

and $\quad (\gamma+1)^{m_1}(\gamma^2+\gamma+1)^{m_{1\pm1}} = 0 \quad \text{for } 1 < t \leq m$

and +/- accordingly as t is odd/even respectively.

3.7 EIGEN -VECTORS OF THE REED-MULLER MATRICES:

The roots of the characteristic equations of the Reed-Muller matrices, being limited to the three kinds of

roots that may be had and hence their occurance with multiplicity greater than 1, suggests that it may not be feasible to uniquely associate an eigenvector to each root. Eigen-vectors corresponding to multiple roots may be found using the Jordan canonical form of matrices [13]. A more specific method of calculating the eigen-vectors, when the characteristic equation has multiple roots is by the use of the generalised inverse of the characteristic inmatrix of the RM matrix R.

The condition for which non-null solutions of the vector u, may be obtained for $Ru = \gamma u$ is that $(R-\gamma I)$ is singular. For singular matrices, only the first of the four Moore-Penrose conditions for the unique inverse may be satisfied and hence only the generalised inverse may be obtained.

Using this generalised inverses of the characteristic matrix and an arbitrary matrix z, the non-null solution of u may be obtained as

$$u = [(R \oplus \gamma I)^{-} (R \oplus \gamma I) \oplus I] z \qquad (3.7.1)$$

Further, the number of such solutions that $(R-\gamma I)u=0$ may have are determined by the order and rank of the characteristics matrix for that root, which may be written as

$$n-r (R \oplus \gamma I) \qquad (3.7.2)$$

i.e. these may linearly independent eigenvectors may be
obtained and with this as the basis, the entire span of
the eigen-vectors may be had.

The method of obtaining the modal matrix, i.e. the
set of all non-null u as the columns, the algorithm given in
Sec. 2.6 may be used. The characteristic matrix $(R-\gamma I)$ may be
partitioned as

$$R \oplus \gamma_k I = B_k = \begin{bmatrix} R_k & C_K \\ D & E \end{bmatrix} \qquad (3.7.3)$$

for each eigenvalues γ_k, where R_k is non-singular with the
same rank as the characteristic matrix $(R-\gamma_k I)$. And, if R_k
does not satisfy this criteria, then by operating with the
permutation matrices on the characteristic matrix, R_k may
be made to fullfil this condition (Sec. 2.8 refers). Then
the generalised inverse obtained for the characteristic
matrix is

$$(R \otimes \gamma_k I)^- = \begin{bmatrix} R_k^{-1} & 0 \\ 0 & 0 \end{bmatrix} \qquad (3.7.4)$$

Further, considering the arbitrary vector Z and partitioning
it as

$$Z' = [-V, \ W]' \qquad (3.7.5)$$

and substituting in (3.7.1), a number of non-null solution
governed by (3.7.2) for arbitrary w of order $n-r(R-\gamma_k I)$,
is obtained as

$$u_k = \begin{bmatrix} +R_k^{-1}C_k & w \\ \\ w \end{bmatrix} \qquad (3.7.6)$$

The modal matrix so obtained, may be modified to fit the field over which all operations are being implemented to enable obtain the same with ease. The arbitrary matrix w in the modal matrix (3.7.6) may be qualified in an unique manner to ensure that the columns are indeed unique thus giving the $n-r(R-\gamma_k I)$ unique vectors, being the set of linearly independent eigen-vectors. The property of the arbitrary matrix w, therefore would have to be full-column ranked. Such a matrix in GF(2) would be an identity matrix. And, hence the modal matrix for the Reed-Muller matrices may be written as

$$M_k = \begin{bmatrix} (R_k^{-1})(C_k)(I) \\ \\ I \end{bmatrix} = \begin{bmatrix} (R_k^{-1})(C_k) \\ \\ I \end{bmatrix} \qquad (3.7.7)$$

The order of the identity matrix being $n-r(R-\gamma_k I)$ and where R_k is the non-singular submatrix of the characteristic matrix of rank, $r(R-\gamma_k I)$ and the matrix C_k, another submatrix of the characteristic matrix whose rows are the rows of the R_k matrix extended and the columns are the columns remaining from the characteristic matrix after the matrix R_k has been obtained.

This method of obtaining the modal matrix may be applied to both simple and multiple roots and also where the roots are in the extension fields.

Illustrative Example 3.7.1:

For a 2 variables Boolean function with polarity function 11 the RM matrix for the positive canonic RM expansion is

$$R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

and the characteristic matrix is

$$(R-\gamma I) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

the order and rank of the characteristic matrix are 4 and 2 respectively.

$$B_k = \begin{bmatrix} R_k & C_k \\ D & E \end{bmatrix} = \begin{bmatrix} 10 & 00 \\ 11 & 10 \\ 00 & 00 \\ 00 & 00 \end{bmatrix}$$

and R_k being involutory $I_k^{-1} = R_k$

and $R_k^{-1} C_k = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \begin{bmatrix} 00 \\ 10 \end{bmatrix} = \begin{bmatrix} 00 \\ 10 \end{bmatrix}$

and matrix w, which is arbitrary of order $n - r(\imath - \gamma I)$ could be choosen as the identity matrix of this order, viz.

$$w = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$$

and thus

$$M = \mu_k = \begin{bmatrix} R_k^{-1} C_k & w \\ & w \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 00 \\ 10 \end{bmatrix} & \begin{bmatrix} 10 \\ 01 \end{bmatrix} \\ 10 \\ 01 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

illustrative Example 3.7.2:

Considering the 2 variable Boolean-function with polarity function 10. The RM matrix is

$$R = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \otimes \begin{bmatrix} 01 \\ 11 \end{bmatrix} = \begin{bmatrix} 0100 \\ 1100 \\ 0101 \\ 1111 \end{bmatrix}$$

The characteristic matrix

$$(R-\gamma I) = \begin{bmatrix} \gamma & 1 & 0 & 0 \\ 1 & \gamma^2 & 0 & 0 \\ 0 & 1 & \gamma & 1 \\ 1 & 1 & 1 & \gamma^2 \end{bmatrix}$$

the rank of the characteristic matrix is

$$r(R-\gamma I) = 3$$

Therefore there are $n-r(R-\gamma I)$ LIN EVS which is $4-3=1$.

Partitioning the characteristic matrix, after permuting

we obtain

$$B = \begin{bmatrix} 1 & \gamma^2 & 0 & 0 \\ 0 & 1 & \gamma & 1 \\ 1 & 1 & 1 & \gamma^2 \\ \gamma & 1 & 0 & 0 \end{bmatrix} \quad \text{and } R_k = \begin{bmatrix} 1 & \gamma^2 & 0 \\ 0 & 1 & \gamma \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and } C_k = \begin{bmatrix} 0 \\ 1 \\ \gamma^2 \end{bmatrix}$$

for the root $\gamma = \alpha$

$$R_k{}^{-1} = \begin{bmatrix} \alpha & \alpha & \alpha^2 \\ 1 & \alpha^2 & 1 \\ \alpha^2 & 1 & \alpha^2 \end{bmatrix}_{\gamma=\alpha} \quad \text{with } w = [1]$$

and hence the model matrix for $\gamma = \alpha$

$$M = \begin{bmatrix} \alpha & \alpha & \alpha^2 & 0 \\ 1 & \alpha^2 & 1 & 1 \\ \alpha^2 & 1 & \alpha^2 & \alpha^2 \\ & (1) & & \end{bmatrix}_{\gamma=\alpha} = \begin{bmatrix} 0 \\ 0 \\ \alpha^2 \\ 1 \end{bmatrix}$$

which indeed is an eigenvector.

for $\gamma = (1+\alpha)$ the eigenvectors may be found as

$$\begin{bmatrix} 0 \\ 0 \\ \alpha \\ 1 \end{bmatrix}$$

3.7.1 Eigen-vectors of RM Matrix, for the Positive-Canonic RM Expansion:

However, another algorithm for finding the set of LIN eigenvector of the RM matrix which represent the positive canonic Reed-Muller expansion has been developed. This algorithm is based on the concept of null-space of a matrix.

From the definition of eigenvalues and eigenvectors given in Section 2.6, viz.

$Ru = \gamma u$ for u a vector and γ scalar

it may be written as

$$(R - \gamma I)u = 0$$

and all vectors u that satisfy this condition forms the modal matrices, with the vectors being the columns of this matrix. The null space of a matrix may be defined as the set of all column matrices x which satisfies the homogenous linear equations $Bx = 0$. An easier approach to obtain the null space of the matrix is by making the matrix B full row-ranked and finding a matrix C which satisfies $B'C'=I$

and taking those columns that satisfy Bx=0, the null-space may be obtained. For a matrix $B = (R-\gamma I)$ this may be written as

$$B' = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix} \text{ and } C' = [C_1 C_2] \qquad (3.7.8)$$

such that

$$B_1 C_1 \oplus B_2 C_2 = I \qquad (3.7.9)$$

or equivalently the same equation may be written as,

$$\begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} \qquad (3.7.10)$$

or those C_{12} and C_{22} that satisfy the conditions

$$B_{11} \cdot C_{12} \oplus B_{12} C_{22} = 0 \qquad (3.7.11)$$

$$\text{and } B_{21} \cdot C_{12} \oplus B_{22} C_{22} = I$$

such that $C_2 = \begin{bmatrix} C_{12} \\ C_{22} \end{bmatrix}$ forms the modal matrix $\qquad (3.7.12)$

of the matrix R and being the null-space of the characteristic matrix $(R-\gamma I)$.

It is observed that for $C_{12} = Q$ and $C_{22} = I$ of appropriate order, the modal matrix may be formed. The choice of Q and I also depends on the choice of B_{21} and B_{22} which satisfy the conditions

$$B_{21} \cdot C_{12} \oplus B_{22} \cdot C_{22} = I \qquad (3.7.13)$$

and

$$B_{21} \cdot C_{11} \oplus B_{22} \cdot C_{21} = 0$$

The matrix B_2 may be chosen arbitrarily, with the condition that the matrix B' is full-row ranked . Formats of matrix B, always suggests that the LIN vector of B_2 may be obtained as $[B_{21}, B_{22}]$ by choosing B_{21} as the null matrix and B_{22} as the identity matrix of appropriate order, i.e.

$$0 \cdot Q \oplus I \cdot I = I \text{ is satisfied}$$

and hence the resulting modal matrix takes the form $M = \begin{bmatrix} Q \\ I \end{bmatrix}$, where Q is of the order n/2, n being the order of the Reed-Muller matrix R and Q also takes the same form as the characteristic matrix R, and I is of the order n/2. The identity that

Rank + Nullity = Order is also verified as a result of this.

The matrix Q in the modal matrix M, may also be defined as the matrix Q, the characteristic matrix, with $\gamma=1$, and is of order n/2 or the same may be obtained as the characteristic matrix, with $\gamma=1$, for matrix R', obtained as a direct-product of the core matrix $\begin{bmatrix} 10 \\ 11 \end{bmatrix}$ (m-1) times and I is the identity matrix of order n/2. Alternatively, Q may be written $[R' \rightarrow I]$. The span of the column vectors of the modal-matrix

as the basis v..ctors, the complete set of eigen-vectors of the RM matrix may be found.

Illustrative Example 3.7.3:

Given that the no. of variables in the switching function, m=2.

The c_is for the expression

$$f(x_1,x_0) = c_0\ t_0 \oplus c_1 t_1 \oplus c_2 t_2 \oplus c_3 t_3$$

where t_is are the minterms and c_i {0,1}, indicates whether the function value is zero or one for the related input and as the minterms are disjoint, the inclusive OR, operation is replaced by the exclusive OR operation. For this example let the c_is be 01 01. The other sets of c_is of all possible 2^m values that this may take are the sixteen combinations of 1s and 0s, from 0000 through 1111.

The transform matrix, R for this example is

$$R = \begin{bmatrix}10\\11\end{bmatrix} \otimes \begin{bmatrix}10\\11\end{bmatrix} = \begin{bmatrix}10\ 00\\11\ 00\\10\ 10\\11\ 11\end{bmatrix} \text{ or } \begin{bmatrix}10\ 00\\00\ 10\\11\ 00\\00\ 11\end{bmatrix}^2$$

and the eigenvalues are

$$\begin{matrix}1\\1\end{matrix} \otimes \begin{matrix}1\\1\end{matrix} = \begin{matrix}1\\1\\1\\1\end{matrix} \quad \text{i.e. } \gamma=1, m_1 = 4.$$

To find the modal matrix, we like to find the null space
of characteristic matrix, which in the simplified form is
$\begin{bmatrix} Q \\ I \end{bmatrix}$

$$Q = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and $\quad M = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$

and the set of all eigen-vectors

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

The characteristic matrix of the transform matrix R,

is $(R-\gamma I) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ and then

find the null-space the matrix B so obtained

i.e. $B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ and obtain the set of $\underline{x}_i$ such that

$$Bx = 0$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

and $B' = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}$ may be obtained as $\begin{bmatrix} 1000 \\ 1110 \\ 0010 \\ 0001 \end{bmatrix}$

and obtain c_2 of $c' = [c_1 c_2]$, we may write it as

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

$c_{12} \begin{bmatrix} 10 \\ 11 \end{bmatrix} + c_{22} \begin{bmatrix} 00 \\ 10 \end{bmatrix} = \begin{bmatrix} 00 \\ 00 \end{bmatrix}$

and $c_{12} \begin{bmatrix} 00 \\ 00 \end{bmatrix} + c_{22} \begin{bmatrix} 10 \\ 01 \end{bmatrix} = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$

$c_{22} = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$

and hence $c_{12} \begin{bmatrix} 10 \\ 11 \end{bmatrix} + \begin{bmatrix} 10 \\ 01 \end{bmatrix} \begin{bmatrix} 00 \\ 10 \end{bmatrix} = 0$

$c_{12} = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \begin{bmatrix} 10 \\ 01 \end{bmatrix} \begin{bmatrix} 00 \\ 10 \end{bmatrix} = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \begin{bmatrix} 00 \\ 10 \end{bmatrix} = \begin{bmatrix} 00 \\ 10 \end{bmatrix}$

(as the matrix $\begin{bmatrix} 10 \\ 11 \end{bmatrix}$ is involutary

$c_2 = \begin{bmatrix} 00 \\ 10 \\ 10 \\ 01 \end{bmatrix}$

Illustrative example 3.7.4:

The number of variable in the positive canonic RM

expansion is given as m=5.

a) The order of RM matrix is $n = 2^m = 32$

b) The modal matrix may be easily constructed as

$$M = \begin{bmatrix} Q \\ I \end{bmatrix} = \begin{bmatrix}
0000 & 0000 & 0000 & 0000 \\
1000 & 0000 & 0000 & 0000 \\
1000 & 0000 & 0000 & 0000 \\
1110 & 0000 & 0000 & 0000 \\
1000 & 0000 & 0000 & 0000 \\
1100 & 1000 & 0000 & 0000 \\
1010 & 1000 & 0000 & 0000 \\
1111 & 1110 & 0000 & 0000 \\
1000 & 0000 & 0000 & 0000 \\
1100 & 0000 & 1000 & 0000 \\
1010 & 0000 & 1000 & 0000 \\
1111 & 0000 & 1110 & 0000 \\
1000 & 1000 & 1000 & 0000 \\
1100 & 1100 & 1100 & 1000 \\
1010 & 1010 & 1010 & 1000 \\
1111 & 1111 & 1111 & 1110 \\
1000 & 0000 & 0000 & 0000 \\
0100 & 0000 & 0000 & 0000 \\
0010 & 0000 & 0000 & 0000 \\
0001 & 0000 & 0000 & 0000 \\
0000 & 1000 & 0000 & 0000 \\
0000 & 0100 & 0000 & 0000 \\
0000 & 0010 & 0000 & 0000 \\
0000 & 0001 & 0000 & 0000 \\
0000 & 0000 & 1000 & 0000 \\
0000 & 0000 & 0100 & 0000 \\
0000 & 0000 & 0010 & 0000 \\
0000 & 0000 & 0001 & 0000 \\
0000 & 0000 & 0000 & 1000 \\
0000 & 0000 & 0000 & 0100 \\
0000 & 0000 & 0000 & 0010 \\
0000 & 0000 & 0000 & 0001
\end{bmatrix}$$

CHAPTER 4

GENERATION OF FEED-MULLER EXPANSION COEFFICIENTS

Developing algorithms, which synthesise any arbitray switching function, using a minimum number of logic circuit has been a perpetual problem in switching theory. Boolean realisation use AND/OR/NAND and NOR gates, whereas these functions may also be implemented using Exclusive OR gates. The advantages of designing with Exclusive OR gates, were outlined in Sec. 1.1. Applications using Ex-OR gate realisation has suffered because there are not many algorithms that may be easily applied to find the minimum solution, as are available in the case of Boolena vertex realisations. In the exclusive-OR realisation for the minimum design, it is desirable to minimise the number of terms, in exactly the same manner that it is desirable to minimise the number of prime complicants (AND) terms in a conventional Boolean realisation.

Eigen structure of any matrix characterises the matrix and therefore it is possible to associate the eigen-structure of the Reed-Muller matrices, obtained in the previous chapter, in the generation of the positive canonic and non-positive canonic Reed-Muller expansion coefficients. Thus the eigenstructure of the expansions is able to relate the mintern coefficients (obtained from the truth tables of the Boolean function) to positive canonic and non-positive canonic RM expansion coefficients.

The algorithms developed here are for the two different RM matrices. In the algorithm, for the positive canonic RM expansion, eigenvectors partions the complete set of minterm coefficients vector space C, into cosets and by associating the coset leader with an eigen vector, the positive canonic RM expansion coefficients may be obtained. The other algorithm, makes use of the eigenvalue of the non-positive canonic RM matrices and is able to associate the minterm coefficients to its corresponding non-positive canonic RM expansion coefficient for a given polarity function of the Boolean function.

Both the algorithms may be programmed, when the matrices cannot be handeld i.e. for Boolean functions with large number of variables, and may be employed profitably in the minimisation problems.

4.1 PURPOSE OF GENERATION OF THE NON-POSITIVE CANONIC RM EXPANSION COEFFICIENTS

The generalised Reed-Muller (GRM) expansion may be expressed as (1.7)

$$f(\dot{x}_1, \dot{x}_2, \ldots, \dot{x}_m) = a_0 + a_1 \dot{x}_1 + a_2 \dot{x}_2 +$$
$$+ a_{2^m-1} \dot{x}_1 \dot{x}_2 \ldots \dot{x}_m.$$

where each $\dot{x}_1$ input variable may appear in positive or negative form but not in both forms.

The number of zero-valued a_i coefficients in the
GRM expansions for any given function $f(x)$ and hence the number
of remaining AND and Exclusive terms in the resulting reali-
sation, will vary depending upon the chosen polarity of each
x_i input variable. The extreme polarities of positive and
negative do not contain more zerovalued terms than some other
non-positive canonic RM expansions. Hence the criterion for
minimisation is the selection of that non-positive canonic
expansions which has the maximum number of zero (minimum
number of non-zero) a_i coefficients in the expansion. A com-
parison of all possible non-positive canonic RM expansions are
involved in order to determine a minimum non-positive canonic
RM expansion [21], [22], [23], [27]. It is difficult to
generate these 2^m positive and non-positive canonic RM ex-
pansions and these are not intutive either. Constraints
on the variable being complemented may give rise to minimum
solution. A method has been developed [7], where geometric
plotting and grouping have been outlined and thus after manu-
pulating the coefficient values, a minimised non-positive
canonic RM expansion may be achieved without involving
exhasutive search procedure. A computerised in place algo-
rithm has also been devised [10]. The algorithm enables
sequentially generate all non-positive canonic RM expansion
coefficients, and the algorithm being fast, an exhaustive
search for the minimum is feasible.

The table below clearly shows the advantage of the non-positive canonic RM expansions.

TABLE 4.1.1

LOGIC GATE REQUIREMENTS FOR POSITIVE AND NON-POSITIVE CANONIC RM EXPANSION IMPLEMENTATION

S. No.	Number of variables in the function	Minterm* Coeffs. $f(\dot{x}_1,\dot{x}_2 \ldots \dot{x}_m)$	Positive Canonic RM Expansion			Non-Positive Canonic RM Expansion			Polarity* Pattern of the input variable
			XOR	AND	NOT	XOR	AND	NOT	
1	4	3328	6	5	0	2	2	2	6
2	4	21845 (101010...)	2	1	0	1	0	1	1
3	4	65280 (0...001...11)	1	0	0	1	0	0	0
4	4	43690 (0101...)	1	0	0	1	0	0	0
5	4	255	2	1	0	1	0	1	8
6	5	10000	16	14	0	6 5	6 5	2 4	17 23
7	5	20000	12	12	0	6	6	1	16
8	5	1431655765	2	1	0	1	0	1	1
9	5	227216640	16	14	0	7	6	3	14
10	5	1671935	2	1	0	1	0	1	8
11	6	10000000000	30	29	0	14	14	4	54
12	6	31241814230	34	30	0	12	12	4	60
13	6	30137694138	36	32	0	14	14	5	61
14	6	1234507890	20	18	0	10	10	1	32
15	6	1020304050	28	24	0	11	11	2	40

* Decimal value of the binary representation of the minterm coefficients and the polarity function. When the pattern of minterm coefficients is not indicated, then it is a random pattern.

Minimisation criterion, depending on the realisation may be applied ; one is to minimise the number of AND gates, another one is to minimise the overall number of inputs to the Ex-OR gates or to minimise the overall number of inputs. However, the choice of criterion being the economical implementation of the situation to which the design is to be applied. The penalty to be paid for the non-positive canonic RM expansion implementation is the sub-optimum number of product terms, while the number of input variables or the number of inverters required is generally less than for the minimum form [10].

4.2 GENERATION OF POSITIVE CANONIC RM EXPANSION COEFFICIENTS USING EIGENVALUES

The vector space of all combinations of possible values that c_i s may take get partioned by the eigenvectors of the transform into subgroups, and the RM coefficients for a particular subgroup are governed by a particular eigenvector. Thus it is observed that this vector space is partioned into cosets and the elements of the subgroup or the coset is invariant i.e. the RM expansion coefficient is found from within the coset, governed by an eigenvector.

Thus if h_1, h_2, ... h_n are the eigenvectors of the transform, then cosets may be formed as shown (all operations are modulo 2 addition)

$$
\begin{array}{cccccc}
h_1 & h_2 & h_3 & \cdots & & h_n \\
g_1 \oplus h_1 & g_1 \oplus h_2 & g_1 \oplus h_3 & \cdots & & g_1 \oplus h_n \\
g_2 \oplus h_1 & g_2 \oplus h_2 & g_2 \oplus h_3 & \cdots & & g_2 \oplus h_n \\
& & \vdots & & & \\
g_k \oplus h_1 & g_k \oplus h_2 & g_k \oplus h_3 & \cdots & & g_k \oplus h_n
\end{array}
$$

and in this all $g_1 \oplus h_1$ s become to coset leader. While
forming the cosets, instead of $g_1 \oplus h_1$ being any element that
has not appeared earlier, it is the next lowest element after
h_1, that has not appeared earlier. Thus the coset leader is
the minimum vector in the coset. In the algorithm bit-by-bit
modulo 2 addition of all eigenvectors to the c_is gives the
entire coset and by choosing the minimum vector the coset·
leader is thus obtained.

Now after identifying the coset leader, the eigen-
vector that relates the c_is to the RM expansion coefficient
may be found by multiplying the coset leader with the charac-
teristic matrix of the transform. Having found the eigen-
vector that relates the c_is to the RM expansion coefficient,
a mere bit-by-bit addition of c_i to the eigenvector gives the
RM expansion coefficients.
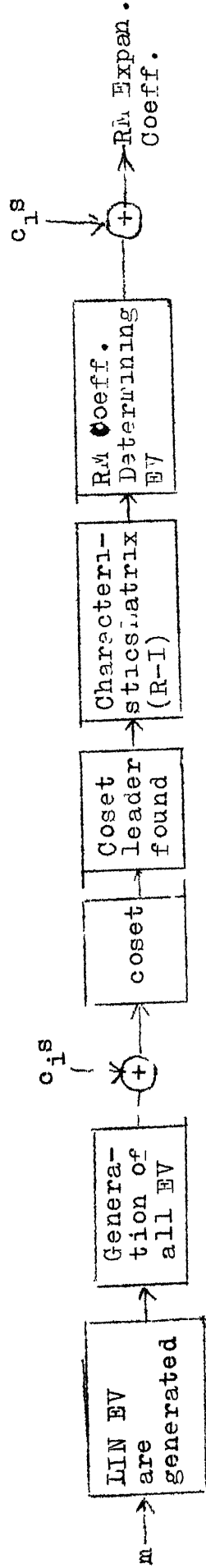
Fig. 4.2.1

The algorithm is schematically depicted above.

Illustrative Example 4.2.1

The cosets for m = 2 could be written as shown below
(the decimal value of c_is are given for ease of notation).

Coset Leader →	0	3	2	1	
↓	0	6	8	14 ← Eigenvectors ↓	
1	1	7	9	15	14
2	2	4	10	12	8
3	3	5	11	13	6

Thus for the given c_i 0101, which is notationaly 10,
(Ten) by carrying out the bit-by-bit operation on all eigen
vectors we get 10, 12, 2 and 4, the minimum of which is 0100,
which is 2, the coset leader also. Now carrying out a vector
matrix multiplication, i.e. the coset leader and the charact-
eristic matrix,

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

we obtain the RM expansion coefficient determining eigen
vector, which is 0001, and bit-by-bit addition of this to the
c_is gives the RM expansion coefficient.

$$\text{i.e.} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{which is so.}$$

Illustrative Example 4.2.2

The coset formation for a 3 variable function is shown in the table. The coset formation contains all the 2^n possible combination which the set of c_is, the minterm coefficients could take. Hence once the table is formulated and the appropriate coset leader associated with the corresponding eigenvector, using the algorithm; the table is available as a ready reference or as a mere look-up table. The effort therefore is only to do a bit-by-bit addition, modulo 2, of the minterm coefficients with the corresponding eigenvector to give the Reed-Muller expansion coefficients. However, in this table the positive canonic RM expansion coefficients, corresponding to each minterm coefficient is also given as the denominator to it i.e. after the vector obtained as a result of bit-by-bit addition of the minterm coefficient with the positive RM expansion coefficient determining eigenvector found from the table.

TABLE 4.2.1
COSET LEADER, EIGENVECTOR LOOK-UP TABLE

Coset Ldr.	0/0	15/30	10/40	5/54	12/72	3/86	6/96	9/126	8/128	7/158	2/168	13/182	4/200	11/214	14/224	1/254	Eigenvectors
1	1/255	31/225	41/215	55/201	73/183	87/169	97/159	127/129	129/127	159/97	169/87	183/73	201/55	215/41	225/31	255/1	254
2	2/170	28/180	42/130	52/156	74/226	84/252	98/202	124/212	130/42	156/52	170/2	180/28	202/98	212/124	226/74	252/84	168
3	3/85	29/75	43/125	53/99	75/29	85/3	99/53	125/43	131/213	157/203	171/253	181/227	203/157	213/131	227/181	253/171	86
4	4/204	26/210	44/228	50/250	76/212	82/154	100/172	122/178	132/76	154/82	172/100	178/122	204/4	210/26	228/44	250/50	200
5	5/51	27/45	45/27	51/5	77/123	83/101	101/83	123/77	133/179	155/173	173/155	179/133	205/251	211/229	229/211	251/205	54
6	6/102	24/120	46/78	48/80	78/46	80/48	102/6	120/24	134/230	152/248	174/206	176/208	206/174	208/176	230/134	248/152	96
7	7/153	25/135	47/177	49/175	79/209	81/207	103/249	121/231	135/25	153/7	175/49	177/47	207/81	209/79	231/121	249/103	158
8	8/136	22/150	32/160	62/190	64/192	94/222	104/232	118/246	136/8	150/22	160/32	190/62	192/64	222/94	232/104	246/118	128
9	9/119	23/105	33/95	63/65	65/63	95/33	105/23	119/9	137/247	151/233	161/223	191/193	193/191	223/161	233/151	247/137	126
10	10/34	20/60	34/10	60/20	66/106	92/116	106/66	116/92	138/162	148/188	162/138	188/148	194/234	220/244	234/194	244/220	40
11	11/221	21/195	35/245	61/235	67/149	93/139	107/189	117/163	139/93	149/67	163/117	189/107	195/21	221/11	235/61	245/35	214
12	12/68	18/90	36/108	58/114	68/12	90/18	108/36	114/58	140/196	146/218	164/236	186/242	196/140	218/146	236/164	242/186	72
13	13/187	19/165	37/147	59/141	69/243	91/237	109/219	115/197	141/59	147/37	165/19	187/13	197/115	219/109	237/91	243/69	182
14	14/238	16/240	38/198	56/216	70/166	88/184	110/142	112/144	142/110	144/112	166/70	184/88	198/38	216/56	238/14	240/16	224
15	15/17	17/15	39/57	57/39	71/89	89/71	111/113	113/111	143/145	145/143	167/185	185/167	199/217	217/119	239/241	241/239	30

The above table also gives the positive canonic RM expansion coefficients. The denominator of each of the minterm coefficient entry is the positive canonic RM expansion coefficient corresponding to it.

Illustrative Example 4.2.3

The number of variables in the positive canonic RM expansion is given as $m = 4$.

(a) The order of the RM matrix is $n = 2^m = 16$

(b) The modal matrix may be obtained as

$$R = [\tfrac{Q}{I}] = \begin{bmatrix} 00000000 \\ 10000000 \\ 10000000 \\ 11100000 \\ 10000000 \\ 11001000 \\ 10101000 \\ 11111110 \\ 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000010 \\ 00000001 \end{bmatrix}$$

The above linearly independent eigenvectors as the basis, the span of these vectors may be found to be consisting of the 256 eigenvectors of the RM matrix. There are 2^n possible combinations of the minterm coefficients i.e. $2^{16} = 65536$. So instead of handling this many combinations, we may store only

the 256 eigenvectors of the RM matrix and by bit-by-bit addition of the given minterm coefficient to these 256 eigenvectors and picking the minimum vector, the coset leader is obtained. The 256 eigenvectors are given at Appendix A

The process of associating the expansion coefficient determining eigenvector to the coset leader could be available as a look-up table, as this is independent of any operations with minterm coefficient and therefore once the coset leader is obtained, then by identifying the expansion coefficient determining eigenvector, bit-by-bit addition of the minterm coefficients gives the corresponding RM expansion coefficients.

This algorithm is very efficient, provided the two look-up tables are available before hand viz. the set of all eigenvectors and the coset-leader to eigenvector table, then with only two sets of bit-by-bit additions, the RM expansion coefficient may be obtained. In general, $2^{n/2} + 1$ bit-by-bit addition and the process of picking the coset leader is adequate and the coset leaders could also be stored in memory for comparision and thus speed-up the operations. The number of coset leader being the total number of eigenvectors itself.

4.3 GENERATION OF NON-POSITIVE CANONIC RM EXPANSION COEFFICIENTS, USING EIGENVALUES

To enable relate the c_is to the positive and non-positive canonic RM expansion an algorithm has been developed,

which is schematically shown below
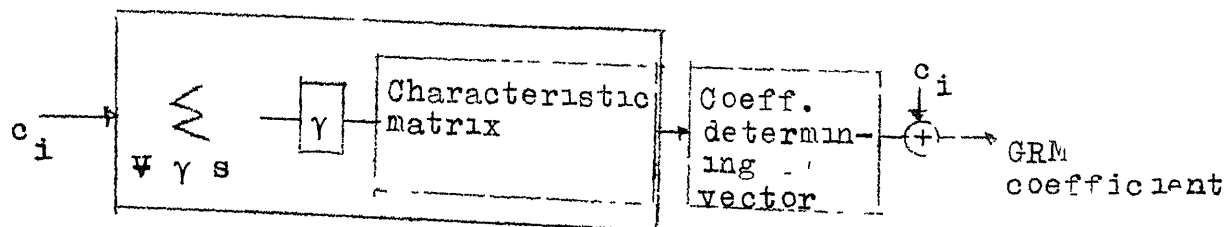
This algorithm may be seen as a version of the one presented in the earlier section and this being applicable to the more general case may be applied to the 'positive' polarity RM expansion coefficients also.

This algorithm may be written as

$$[\underset{\forall \gamma}{\lessgtr} \gamma (R + \gamma I)] - [X] + [X] = RX$$

There are three kind of eigenvalues that are obtainable from the RM matrices viz. $\gamma = 1$, $\gamma = \alpha$ and $\gamma = 1 + \alpha$; also it was mentioned in section 3.2 that whenever $\gamma = \alpha$ occurs then $\gamma = 1 + \alpha$ also occurs. The total number of eigenvalues is 2^m and thus the number of eigenvalues that appear for $\gamma = 1$, if they occur, is always even. It must be remembered that all arithmetic is modulo 2 and therefore the summation of $\gamma(R-\gamma I)$ for all γs, as far as $\gamma = 1$ is concerned may be omitted and evaluating for $\gamma = \alpha$ and $\gamma = 1 + \alpha$, we obtain.

$$LHS = [\alpha(R + \alpha I) + (1 + \alpha)(R + (1 + \alpha) I)][X] + [X]$$

$$= [\alpha R + \alpha^2 I + (1 + \alpha) R + (1 + \alpha)^2 I][X] + [X]$$

$$= [\alpha R + I + \alpha I + R + \alpha R + \alpha I] \ [X] + [X]$$

$$= [I + R] \ [X] + [X]$$

$$= X + R \ X + X = RX = RHS \qquad QED.$$

It is observed that weighting the characteristic matrix by the root results in the characteristics matrix, which is what has been used in the previous algorithm. In this algorithm instead of obtaining the eigenvectors that determines the RM expansion coefficients, some arbitrary vector is obtained, which determines the GRM expansion coefficients.

Illustrative Example 4.3.1

For a 3 variable Boolean function of polarity $\bar{x}_1 \ \bar{x}_2 \ \bar{x}_3$ i.e. m = 3, polarity = 101

$$\therefore R = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \times \begin{bmatrix} 01 \\ 11 \end{bmatrix} \times \begin{bmatrix} 10 \\ 11 \end{bmatrix}$$

$$= \begin{bmatrix} 00100000 \\ 00110000 \\ 10100000 \\ 11110000 \\ 00100010 \\ 00110011 \\ 10101010 \\ 11111111 \end{bmatrix} = \begin{bmatrix} 10000000 \\ 00100000 \\ 00001000 \\ 00000010 \\ 11000000 \\ 00110000 \\ 00001100 \\ 00000011 \end{bmatrix} \begin{bmatrix} 01000000 \\ 00010000 \\ 00000100 \\ 00000001 \\ 11000000 \\ 00110000 \\ 00001100 \\ 00000011 \end{bmatrix} \begin{bmatrix} 10000000 \\ 00100000 \\ 00001000 \\ 00000010 \\ 11000000 \\ 00110000 \\ 00001100 \\ 00000011 \end{bmatrix}$$

for the given set of c_i say 10011001, we may obtain the GRM expansion coefficients as

$$a = R^{\sim} c$$

Alternately, we know that there is only one variable being complemented i.e $t = 1$ and we may obtain the number of roots in the ground field and extension field either as direct product of the individual core matrices such as

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ 1+\alpha \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

i.e. $\quad \gamma = \alpha \; ; \; m_\alpha = 4$

$\qquad \gamma = 1 + \alpha \; ; \; m_{1+\alpha} = 4$

or using the formula we have

$m = 3$, $t = 1$ therefore there are no roots in the ground field and all roots are in the extention field and there are $d = 2^m$ of them i.e. 8, 4 of them are $\gamma = \alpha$ and the other 4 are $\gamma = 1+\alpha$ (or α^2)

The characteristic equation is

$$(\gamma^2 + \gamma + 1)^{m_\alpha} = 0$$

i.e. $\quad (\gamma^2 + \gamma + 1)^4 = 0$

Now using the algorithm the GRM expansion coefficients can be found as follows :

$$a = [\underset{\neq \gamma_\Delta}{\leqq} \gamma(R \not{+} \gamma I)][c] \oplus [c]$$

$$a = \alpha \begin{bmatrix} \alpha & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & \alpha^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \alpha & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & \alpha & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & \alpha^2 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha^2 \end{bmatrix} \oplus (1 \oplus \alpha) \begin{bmatrix} \alpha^2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^2 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & \alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \alpha^2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & \alpha^2 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & \alpha & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix} \oplus \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix}$$

and simplifying over the irreducible polynomial,

$$= \begin{bmatrix} 10100000 \\ 01110000 \\ 10000000 \\ 11100000 \\ 00101010 \\ 00110111 \\ 10101000 \\ 11111110 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix} \oplus \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix}$$

$$\begin{bmatrix} c_1 \oplus c_3 \\ c_2 \oplus c_3 \oplus c_4 \\ c_1 \\ c_1 \oplus c_2 \oplus c_3 \\ c_3 \oplus c_5 \oplus c_7 \\ c_3 \oplus c_4 \oplus c_6 \oplus c_7 \oplus c_8 \\ c_1 \oplus c_3 \oplus c_5 \\ c_1 \oplus c_2 \oplus c_3 \oplus c_4 \oplus c_5 \oplus c_6 \oplus c_7 \end{bmatrix} \oplus \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix}$$

$$\begin{bmatrix} c_3 \\ c_3+c_4 \\ c_1+c_3 \\ c_1+c_2+c_3+c_4 \\ c_3+c_7 \\ c_3+c_4+c_7+c_8 \\ c_1+c_3+c_5+c_7 \\ c_1+c_2+c_3+c_4+c_5+c_6+c_7+c_8 \end{bmatrix}$$

which for the given set of c_is viz. 10011001, is

$$a^T = [\,01100000\,]$$

and thus the required GRM expansion coefficients have been found for the polarity 101.

4.4 GENERATION OF THE RM EXPANSION COEFFICIENTS BASED ON GOOD'S FACTORISATION OF THE RM MATRICES

An 'm' variable Boolean function could have any polarity for specified optimum solution. As already mentioned 'in-place' computer algorithm [10] is available for this. The program given at Appendix B too, though not 'in-place', gives the same results, with the flexibility that even for any random polarity the non-positive canonic RM expansion coefficients may be had in a single run. The Reed-Muller matrix is built-up as Kronecker product and then factorised as two kinds of matrices using Good's technique, which when sequentially processed gives the desired positive/non-positive canonic

RM expansion coefficients. As the representation in the program for the matrix is the existence or otherwise of an '1' element in the matrix, the computation is also fast i.e. only the location of the elements in the matrices determines the output vector. The Reed-Muller matrix is thus factorised as

$$R = R_{x_1} \cdots\cdots\cdots R_{x_m}$$

with R_{x_i} taking one of the two formats depending on whether the variable is true or complemented. The program in its present form scans all the possible 2^m polarity functions in a binary sequence and from this the minimum number of AND gates or inputs to Exclusive OR gates or with any other specifications, the desired optimum polarity may be had. The limitation of this program is the capability of the computer/to handle matrices. The program is given at Appendix B .

The minterm coefficients for a 5 variable Boolean function is given as the input. These minterm coefficients are the same used in [10] for the example there. The output may be had in two forms, one as a summary of the number of gates required for each polarity function which is reproduced as a table here, the other besides giving the above data gives the details of RM expansion coefficients, a_is for each

case. The program in its present form does not give the
exact number of Ex-OR gates required, though the same may be
construed and neither does it indicate the type of the AND
gates required i.e. how many input AND gates. However, an
analysis of a_is, the RM expansion coefficients would divulge
the number of inputs to each AND gate.

TABLE 4.4.1

RM EXPANSION COEFFICIENTS FOR DIFFERENT POLARITY OF THE
VARIABLES OF A BOOLEAN FUNCTION

B-J Super-script	Number of input to ExOR gates	Number of AND gates	Number of Invertors (NOT gates)	Remarks
0	16	14	0	
1	14	13	1	
2	12	11	1	
3	14	12	2	
4	9	9	1	
5	11	11	2	
6	8	8	2	
7	13	12	3	
8	17	14	1	
9	16	14	2	
10	12	10	2	
11	16	13	3	
12	9	8	2	
13	10	10	3	
14	7	6	3	
15	11	10	4	
16	20	17	1	
17	18	15	2	
18	18	15	2	
19	16	14	3	
20	13	12	2	
21	17	15	3	
22	14	13	3	
23	21	17	4	
24	16	14	2	
25	16	13	3	
26	14	12	3	
27	14	12	4	
28	10	9	3	
29	12	12	4	
30	10	9	4	
31	14	12	5	

4.5 GENERATION OF MINTERM COEFFICIENTS FROM A GIVEN RM EXPANSION COEFFICIENTS, FOR THE GIVEN POLARITY

The linear transformation from the minterm coefficients to the RM expansion coefficients was represented by the RM matrices. The expression being

$$a = Rc \qquad (4.5.1)$$

Therefore from the given set of non-positive canonic RM expansion coefficients, the minterm coefficients may be obtained as

$$c = R^{-1} a \qquad (4.5.2)$$

The RM matrices were obtained as direct product of core matrices, and structure of the inverse of the RM matrices is also obtained as direct product of the inverses of the core matrices. The inverse of the core matrix is the core matrix itself, the core matrix being involutary. The inverse of the core matrix, for a complemented variable is

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad (4.5.3)$$

and therefore the inverse of the RM matrices are obtained as, direct-product of these inverses combined as per the polarity function of the input variables. Thus for a polarity function 101001, the R^{-1} is

$$R^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad (4.5.4)$$

Illustrative Example 4.5.1

For the 3 variable Boolean function considered
earlier, with polarity function 110, the non-positive canonic
RM expansion coefficients were obtained as

$$[a]^T = [01100000]$$

The matrix R^{-1} may be obtained as

$$R^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Therefore the minterm coefficients may be obtained as

$$c = \begin{bmatrix} 11000000 \\ 10000000 \\ 11110000 \\ 10100000 \\ 11001100 \\ 10001000 \\ 11111111 \\ 10101010 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

which is $[c]^T = [10011001]$

These were the minterm coefficients originally assumed
in the example and therefore R^{-1} may be obtained as mentioned
in this section.

CONCLUSIONS AND SUGGESTIONS FOR FURTHER RESEARCH

5.1 SUMMARY OF THE THESIS:

Minimising the number of logical circuit elements
has always been a problem. Various techniques such as
Karnangh map and Quine McClusby's technique, and the
recent 'b$_J$ mapping' help achieve a limited aim. The
search was for more economical realisation and therefore
designing only with exclusive-OR and .ND gates were
adopted, (in addition, inverters. too would be required).
This gave rise to the problem of minimisation of the Ex-OR gates a
gates and the parameters on which this minimisation has
been defined is the polarity function of the variables of
the Boolean function. So the Boolean function, **via** its
minterm coefficients could be related to which came to be
known as the RM expansion coefficients. The transformation
was accordingly termed as the RM matrix.

The RM matrices were obtained on direct-product, of
core matrix and thus the eigen-values could be easily
obtained as direct-product. The problem of multiple roots
of the characteristic equation, especially, in the case of
the RM matrix for the positive canonic RM expansion was
simplified and the eigen-values of the RM matrices for the

non-positive canonic RM expansions were formulated, again as a function of the polarity function of the input variables. As the RM matrices could be obtained as direct-product of core-matrices, they could also be factorised by Good's technique. The main advantage of this factorisation has been that the few non-redundant entries in a matrix   could be made fewer, resulting in fewer number of operations for the transformation implementation. This aspect has been exploited utmost for computer implementation of the generation   of the RM expansion coefficients.

The purpose of generation of RM expansion coefficients itself was considered essential for minimisation of the Ex-OR designs. The eigen-structure of the RM matrices were used for the   generation   of the RM expansion coefficients. Good's technique of factorisation was also put to use.

The main dark area in   the use of Ex-OR design has been that not many usable algorithms are available. This thesis is an effort to contribute towards understanding the problem and try and give an easier approach to it. Table 4.1.1/Chapter 4 would evince   the circuit designers into thinking   of designing chips, though may be exclusively dedicated, but extremely small in size. However, the economical production of the 'chips' would be the deciding factor .

5.2 SUGGESTION FOR FUTHER RESEARCH:

The eigenvectors of the RM matrices, for the positive canonic RM expansion, could be used to form lookup tables and thus by a more bit-by-bit addition, of the minterm coefficients with the expansion coefficient determining eigenvector, the expansion coefficient could be obtained. Similar lookup tables could be formed for the RM matrices, for the non-positive canonic RM expansions, so that the non-positive RM expansion coefficients too could be obtained in a simple manner.

Practical designing of the circuits, using Exclusive-OR gates, AND gates and invertors could be profitably worked out. The algorithm developed in this thesis or [10] , could be put to use.

Lastly, every digital information processing essentially being represented by a set n function of m variables on the GF(2), such a set of functions could be reduced to one polynomial of one variable over the extension field, $GF(2^N)$. Such polynomials have remarkable properties, which may be used effectively in designing of switching circuits [28].

REFERENCES

1. Murago S., 'Logic Design and Switching Theory', John Wiley and Co., 1979.

2. Chinal J., 'Design Method for Digital Systems', Springer-Verlog, Berlin, 1967.

3. Reed IS, 'A class of Multiple-error Correcting Code and the Decoding Scheme', IRE Trans. 1954, IT-4, pp. 38-49.

4. Muller DE, 'Applications of Boolean Algebra to Switching Circuit Design and to Error Detection', IRE Trans. 1954, EC-3, pp. 6-12.

5. Ashenhenhurst RL, 'The Decomposition of Switching Functions', Proc. Intelnl Symp. on the Theory of Switching, Harvard University, 1959, vol. 29, pp. 74-116.

6. Roth and Karp, 'Minimisation over Boolean Graph', IBM Journal Res. and Development 1962, vol. 6, pp. 227-238.

7. Wu, Chen and Hurst, 'Mapping of Reed-Muller Coefficient and the Minimisation of Exclusive-OR Switching Function', IEE Proc. 1982, vol. 129, Pt. E, No. 1, pp. 15-20.

8. Reddy SM, 'Easily Testable Realisation for Logic Functions', IEE Trans. 1972, C 22, pp. 1183-118

9. Birkhoff and MacLane, 'A Survey of Modern Algebra', MacMillan and Co., 1962.

10. Besslich P.D., 'Efficient Computer Method for Exclusive-OR Logic Design', IEE Proc. 1983, vol. 130, Pt. E, No. 6 pp. 303-306.

11. Antan Glaser, 'History of Binary and other Non-decimal Numeration', published by the author Southampton, Penn. USA.

12. Bellman R., 'Introduction to Matrix Analysis' McGraw Hill, New York, 1960.

13. DeRusso, Roy and Close, 'State Variables for Engineers', John Wiley and Sons Inc., 1967, pp. 255-262.

14. Kurosh A., 'Higher Algebra ', (English Translation) Mir Publishers, Moscow.

15. Lanchanster P., 'Theory of Matrices', Academic Press, New York,1969.

16. Pease MC, 'Methods of Matrix Algebra', Academic Press, New York,1965.

17. Peterson WW, 'Error Correcting Codes', MIT Press, 1961.

18. Samuel C. Lee (edited by MINE DC), 'Computer Science and Multilevel Logic Theory and Applications', North-Holland Publishing Co., 1977.

19. Searle SK, 'Matrix Algebra useful for Statistics', John Wiley and Co. 1982.

20. Williams, CE, 'Boolean Algebra with Computer Applications', MacGraw Hill, 1970.

21. Mukhopadhyaya and Schmitz, 'Minimization of Exclusive-Or and Logical Equivalence Switching Circuits', IEEE Trans. 1970, C-19, pp. 132-140.

22. Papakonstantinov G., 'Minimisation of modulo 2 sums-of-products', IEEE Trans. 1979, C 28, pp. 163-167.

23. Kodandapani and Setlur , 'A note on Minimal Reed-Muller Canonic Forms of Switching Functions', IEEE Trans. 1977, C 26, pp. 310-313.

24. Hurst SL, 'Logical Processing of Digital Signals', Edward Arnold, London and Crane Ruasak, New York, 1978.

25. Andrews and Caspari , 'A General Technique for Spectral Analysis', IEEE Trans. 1970, C-19, pp. 16-25.

26. Good IJ, ' The Interaction Algorithm and Practical Fourier Analysis', J. Royal Statistical Society, London, B-20, p. 361, 1958.

27. Saluja and Ong, 'Minimisation of Reed-Muller Canonic Expansions', IEEE Trans. 1979, C-28, pp. 535-537.

28. Takahashi I., 'Switching Functions Constructed by Extension Fields', Information and Control, 1981, vol. 48, pp. 95-108.

EE-1885-M-MON-EIG